


3 1761 11648375 1









Digitized by the Internet Archive  
in 2023 with funding from  
University of Toronto

<https://archive.org/details/31761116483751>







CAL  
ND 800  
-S16

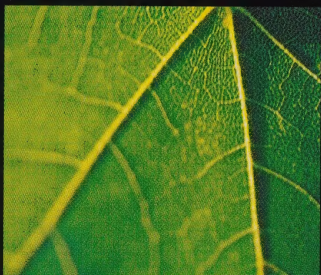


Government  
Publications

149

COMMUNICATIONS  
SECURITY  
ESTABLISHMENT  
COMMISSIONER

# Annual Report



2003-2004

Canada



Office of the Communications Security Establishment Commissioner  
P.O. Box 1984  
Station "B"  
Ottawa, Ontario  
K1P 5R5

Tel.: (613) 992-3044  
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2004  
ISBN 0-662-68250-5  
Cat. No. D95-2004



Communications Security  
Establishment Commissioner



Commissaire du Centre de la  
sécurité des télécommunications

The Right Honourable Antonio Lamer,  
P.C., C.C., C.D., L.L.D., D.U.

Le très honorable Antonio Lamer,  
c.p., c.c., c.d., L.L.D., d.u.

June 2004

Minister of National Defence  
MGen G.R. Pearkes Building, 13th Floor  
101 Colonel By Drive, North Tower  
Ottawa, Ontario  
K1A 0K2

Dear Sir:

Pursuant to sub-section 273.63 (3) of the *National Defence Act*, I am pleased to submit to you my 2003-2004 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Antonio Lamer

P.O. Box/C.P. 1984, Station "B"/Succursale « B »  
Ottawa, Canada  
K1P 5R5  
(613) 992-3044 Fax: (613) 992-4096





## CONTENTS

Introduction .....	1
The Year in Review .....	2
• Governing authorities for foreign intelligence collection.....	3
• Ministerial authorizations .....	5
• Report of the Auditor General of Canada .....	7
2003-2004 Activities .....	8
• Reviews under the Commissioner's general mandate .....	8
• Reviews of activities under ministerial authorizations .....	8
• Review of past recommendations .....	9
• 2003-2004 Findings .....	10
• Complaints and concerns about CSE activities .....	10
The Commissioner's Office.....	11
• Office expenditures and staff .....	11
Looking Ahead .....	13
• New national security policy .....	13
• Proposed legislation.....	14
• Review agencies conference .....	16
Concluding Thoughts .....	16
Annex A: Mandate of the Communications Security Establishment Commissioner .....	17
Annex B: Statement of Expenditures 2003-2004.....	19
Annex C: Classified Reports, 1996-2004.....	21





## INTRODUCTION

This is my first report as Communications Security Establishment (CSE) Commissioner following my appointment on June 19, 2003.

During my twenty years on the Supreme Court of Canada, ten of them as Chief Justice, I witnessed and participated in the evolution of human rights and freedoms in this country, as we grappled with the application and impact of the *Canadian Charter of Rights and Freedoms*. This experience dovetails very well with my duties as CSE Commissioner, because safeguarding the rights of Canadians, including in particular the right to privacy, is an important element, although not exhaustive, of my mandate. In accepting this order-in-council appointment last June, therefore, I was honoured and pleased to have the opportunity to continue serving my country in a meaningful way.

Since retiring from the Court, I have participated in independent reviews and inquiries. One lesson I took from those experiences was the value of working collaboratively when seeking change and reform. With this background, my approach to reviewing the activities of the Communications Security Establishment is essentially proactive and preventive. When reviewing CSE operations to ensure that no unlawful activity has occurred, I also look for the existence of preventive counter-measures to safeguard against situations arising in which unlawful activity *could* occur. In areas as vital as security and intelligence where Canadians' privacy is at stake, I believe this approach is not only warranted but essential in establishing the appropriate balance between the demands of security and intelligence and the privacy rights of Canadians.

Under this approach, if I had concerns as a result of a review conducted by my office, my first step would be to share those concerns with the relevant persons — the Chief of CSE and those who report

to him. This would afford them an opportunity to institute corrective measures or to explain to me why my concerns were unjustified. By proceeding in this way, it is my hope that when I submit classified reports to the Minister of National Defence, most of the problem areas I have identified will already have been addressed, and my report will have been rendered moot.

This approach has proved useful in the past, often resulting in prompt administrative action. As a result, it has been possible to improve the way things are done expeditiously and without confrontation. In this way, the review and reporting process becomes a vehicle not just for detecting unlawful activity but for preventing it in the first place. When constructive criticism is accepted in the spirit in which it is intended, this approach works to the benefit of all concerned.

## THE YEAR IN REVIEW

To prepare myself for the work ahead, in the first few months after my appointment I received several briefings from my own staff and from officials at CSE, including meetings with the Chief and his executive team. I met with the Minister of National Defence as well as his predecessor. I also met with the Security Intelligence Review Committee and with the Security and Intelligence Coordinator, who is also the National Security Advisor to the Prime Minister, and to whom the Chief of CSE reports for matters of operations and policy.

What quickly became apparent to me was the array of challenges facing CSE and the rest of the intelligence community in light of globalized threats with implications for Canada's international affairs, defence and security. The need to monitor and understand these threats is vital, yet efforts to do so have been curtailed in recent years by what has become an increasingly complex web of global communication technologies. Significant



challenges to foreign intelligence collection — one of CSE's primary mandates — also arise in this environment.<sup>1</sup>

These and other new demands led to legislative amendments and the development of new legal frameworks that should meet two objectives: first, facilitating the activities of intelligence agencies; and second, requiring that those agencies meet certain standards and respect certain thresholds that allow them to define and account for their activities.

In parallel with technological development to permit foreign intelligence collection in an ever expanding and complex global communications environment, it is also important to develop technologies that enable intelligence agencies to protect the rights and privacy of Canadians. In other words, technology developed for purposes of acquiring information from the global information infrastructure *must* be complemented by technology that can be used to protect privacy. It is in this context that the need for review of CSE's activities remains high.

Against this backdrop, several general issues related to foreign intelligence collection drew my attention in the past year; two in particular warrant discussion here.

## **Governing authorities for foreign intelligence collection**

Canada's intelligence requirements, including its foreign intelligence priorities, are established annually by the Ad Hoc Committee on Intelligence Priorities (formerly the Meeting of Ministers on Security and Intelligence), chaired by the Prime Minister. Several federal agencies, including the Communications Security Establishment, contribute to meeting these priorities.

---

<sup>1</sup> *Foreign intelligence* is defined in the *National Defence Act* as information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security (Part V.1, section 273.61).

To carry out its foreign intelligence mandate, the CSE relies on the authority of the *National Defence Act (NDA)*,<sup>2</sup> which empowers CSE to “acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities”. When CSE does this, it is acting as a *principal* provider of foreign intelligence.

In addition, CSE, under the authority of the *NDA*, assists other federal agencies in the performance of their lawful duties. In these instances, CSE does so as an *agent*. In providing technical and operational assistance to federal law enforcement and security agencies, CSE is strictly governed by the terms and conditions of the principal’s governing authorities, which in some instances may be a warrant from the Federal Court of Canada.

These two roles — as principal and agent — were formalized in legislation in 2001, but they are not new for CSE. What is new is CSE’s authority under the *NDA* to intercept private communications under prescribed conditions, if authorized to do so by the Minister of National Defence.<sup>3</sup> With a ministerial authorization, CSE can intercept and use a communication with a connection to Canada (that is, a ‘private communication’) acquired in the course of targeting a foreign entity abroad, provided it meets certain conditions laid out in the

---

<sup>2</sup> R.S.C. 1985, c. N-5.

<sup>3</sup> *Private communications* are the communications of Canadians or persons in Canada. Specifically, *private communication* is defined in section 183 of the *Criminal Code* as any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.

---

*NDA*. This provision adds a new authority to the legal framework within which foreign intelligence can be lawfully acquired.

From my initial review of some foreign intelligence collection activities, I had concerns that, in some instances, the linkages between these activities and the authorities that govern them were not being given due consideration. I was pleased to learn, therefore, that during the past year the legal frameworks available to the intelligence community for foreign intelligence collection were revisited to ensure that all available authorities had been fully considered before foreign intelligence activities were authorized. I encourage the government to continue to do so.

## **Ministerial authorizations**

Historically, governments have relied on intelligence gathering as part of their efforts to protect and promote national interests and to identify and counter threats to those interests. The advent of new technologies, along with revolutionary developments in the communications industry over the past decade, have hindered some traditional forms of intelligence collection, including the foreign signals intelligence collection performed by CSE.

In the not so distant past, foreign intelligence collection was fashioned around predictable communications patterns and technologies. As a result, it could be conducted within relatively neatly defined legal frameworks. This environment facilitated the review and assessment of foreign intelligence collection activities. During my first year as CSE Commissioner, however, I quickly understood that this is no longer the case. Governments have had to reassess their ability to protect national interests and counter activities such as terrorism that threaten domestic and international security. Canada is no exception.



New legal mechanisms were needed to respond to this changing environment. One response was the ministerial authorization (MA) provisions in Part V.1 of the *National Defence Act*, added to the Act in 2001.<sup>4</sup>

Today's integrated technologies carry different kind of traffic and follow complex communication paths that transit international borders and mix foreign communications with private communications. The MA provisions do not allow CSE to target Canadians or their communications. (CSE has never been allowed to do this.) Today, however, CSE is in a better position to fulfil its foreign intelligence responsibilities because, with the Minister's consent it can follow targeted foreign communications even if they have a connection with Canada. I believe that few Canadians would disagree with the intent of this provision and the authority it provides in today's context of terrorism and threats to Canadians' safety and security.

Since the new legislation was passed, I can confirm that CSE has exercised this authority. As CSE Commissioner, I understand the need for it and support its objective. Subsection 273.65 (8) of the *NDA* requires that I review CSE activities carried out under an MA to ensure that they are authorized and report annually to the Minister.

---

<sup>4</sup> Part V.1 was added to the *National Defence Act* by the *Anti-Terrorism Act*, which became law on December 24, 2001. Before issuing a ministerial authorization, the Minister must be satisfied that the four conditions set out in subsection 273.65 (2) of the *NDA* have been met:

- (a) the interception will be directed at foreign entities located outside Canada;
- (b) the information to be obtained could not reasonably be obtained by other means;
- (c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
- (d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

## Report of the Auditor General of Canada

I believe CSE's policies, instruments and processes must require and facilitate the management and accountability of any activities it conducts under the authority of an MA, particularly activities that relate to intercepting private communications and safeguarding the privacy of Canadians. While this is an evolving process, I can report that CSE has continued to improve the MA structure and strengthened the MA management and accountability mechanisms.

The Auditor General's November 2003 report was tabled in Parliament on February 11, 2004. Chapter 10 of the report — Other Audit Observations — included an audit note, headed *Independent reviews of security and intelligence agencies*, that went on to state, "The activities of security and intelligence agencies are not subject to consistent levels of review and disclosure."

The report suggested that the CSE Commissioner's annual report should be expanded beyond considering CSE's compliance with the law to include such topics as management issues or potential problems at CSE. I believe that a review of the annual reports produced by this office to date will confirm that these areas have, in fact, been considered as they relate to two of the organization's business lines, foreign intelligence collection and the protection of government information systems and networks.

For example, over the past several years, reviews have led to observations in such areas as CSE's strategic planning activities; internal policies, procedures and handling practices; and management and control frameworks. These observations have always been made, however, in the context of lawfulness and CSE's efforts to safeguard the privacy of Canadians.



---

I believe the content of the CSE Commissioner's public annual report must be guided by his mandate, which is to review and report on CSE's activities to ensure that they are in compliance with the law, and to report to the Minister of National Defence annually on the Commissioner's activities and findings.

## **2003-2004 ACTIVITIES**

I submitted a total of five classified reports to the Minister of National Defence over the period covered by this report. Two of these were initiated by my predecessor and completed during the first year of my term.

### **Reviews under the Commissioner's general mandate**

In 2003-2004, I submitted three classified reports to the Minister of National Defence on subjects related to my general mandate to review CSE's activities to ensure they conform with the law.

Submitting a classified report to the Minister does not mean that a lack of compliance with the law or ministerial authority has been detected. It indicates only that the report contains material that requires classified handling. I report to the Minister on all my reviews, either to provide assurance or to bring concerns to his attention, as each specific situation requires.

### **Reviews of activities under ministerial authorizations**

CSE conducted activities under seven ministerial authorizations in 2002-2003; two of these concerned foreign intelligence collection, while five related to information technology security. Within the time frame covered by this report, my office reviewed activities under five of the MAs; the others were nearing completion at the end of the reporting year. The five reviews resulted in two reports to the Minister, both covering information technology security activities.

None of the reports raised issues of unlawfulness.

However, a more general issue about the structure of and process for using ministerial authorizations did arise. Certain weaknesses in policies and procedures related to these activities were brought to CSE's attention. While some issues have been resolved, others remain. I hope to be able to report further on these issues in next year's report.

Annex C provides a list of all classified reports to the Minister submitted by my predecessor and me since the Commissioner's office was established in 1996.

## **Review of past recommendations**

This year my staff reviewed all recommendations made by my predecessor and me in classified reports submitted to the Minister of National Defence since the creation of this office in 1996. The goal was to follow up with CSE on these recommendations and to determine whether the issues identified had been dealt with satisfactorily. I will be asking CSE for an annual update of this information.

The review showed that CSE's response to the recommendations has not been uniform. This is not surprising, given the diverse nature of the recommendations made to date: some could be implemented immediately; some related to policy or procedures; some were of a technical nature; and some required further study to determine their feasibility. Many related to how CSE can better manage and account for its activities.

Based on this review, I would observe that CSE has responded to many of the Commissioner's recommendations, but that a number of issues remain to be addressed, in particular, by establishing work plans and timetables with milestones and completion dates for specific corrective actions that CSE has acknowledged are necessary.

As I have made clear throughout this report, my recommendations and those of my predecessor are intended generally to be preventive, to forestall the

---

possibility of non-compliance by putting effective controls in place. It is in this spirit that I will continue to follow up on CSE's response to recommendations from my office.

## 2003-2004 Findings

I can report that the activities of CSE that my office reviewed during the past year complied with the law and with ministerial authority. It is important to place this assertion in context. It should not be taken to mean that I am certifying that all CSE's activities in 2003-2004 were lawful. I cannot make this assertion, because I did not review all their activities — and no independent reviewer could. However, my office reviews a wide range of activities in considerable depth, based on our assessment of where the risks of unlawful activity are likely to be greatest. This is the appropriate context for the assurance my work provides.

I should add, however, that during the course of reviews, I occasionally identify circumstances where there are clear and evident risks that unlawful activity might occur (arising, for example, from deficiencies in policies or practices). My predecessor and I have made a practice of reporting these circumstances to CSE and to the Minister. As I made clear in the introduction to this report, I believe it is ultimately more useful to prevent unlawful activity than to identify it after the fact.

## Complaints and concerns about CSE activities

There were two complaints in the period covered by this report, but neither led to a formal investigation.

If I am to be in a position to assure complainants that CSE is not engaging in unlawful activity, my approach to complaints must take into account the mandate assigned to CSE under Part V.1 of the *National Defence Act*. Now, as before the introduction of Part V.1, CSE must not target



**THE  
COMMISSIONER'S  
OFFICE**  
**Office expenditures  
and staff**

the communications of Canadians or persons in Canada. As discussed earlier, however, it is no longer possible to state unequivocally that both ends of a communication intercepted by CSE are foreign. CSE can now intercept (though it cannot target) private communications, provided it obtains a ministerial authorization in advance. CSE may also use and retain that communication, provided it adheres to guidelines that are also established in Part V.1 of the *NDA* (see footnote 4).

Any complaint submitted to me about CSE's activities must therefore be examined in this light.

No persons approached me to avail themselves of the public interest defence provisions of the *Security of Information Act*, subparagraph 15 (5)(b)(ii).<sup>5</sup>

Since 1996, when the position was first created, the mandate of the Communications Security Establishment Commissioner — and hence the staff and other resources required to carry out that mandate — have undergone considerable evolution. Between June 1996 and December 2001, the Commissioner's role was twofold: to review CSE's activities to determine whether they conformed with the law, and to receive complaints about the lawfulness of CSE activities.

As discussed at length in previous annual reports and alluded to earlier in this report, two features of the *Anti-Terrorism Act* of December 2001 had a direct bearing on the Commissioner's functions: the review of CSE activities conducted under ministerial authorization and the Commissioner's duties under the *Security of Information Act*.

---

<sup>5</sup> R.S.C. 1985, c. O-5.

---

To fulfil these new responsibilities, my office was allocated additional resources to carry out review activities. A bigger workload and more staff have affected the way we organize and manage our work. For example, our internal policies and procedures for managing the office have been enhanced to reflect the maturation of the organization and the increase in staff during the fiscal year.

We have also paid attention to our work methods. Tools such as a standardized methodology, scope statements, and guidelines structure our reviews of CSE's activities in such a way that all reviewers are working to the same standards of rigour and thoroughness. With the addition of more staff involved in these endeavours, my office has embarked on an initiative to record and document these processes wherever possible.

With a new Commissioner and the evolution of the Commissioner's mandate over the past three years, it was time to look at how my office relates to the broader context in which it operates — in particular the federal government community and the security and intelligence community in Canada and internationally. A communications plan, developed this year with input from key players in Canadian intelligence, will help guide my office through the rapidly evolving intelligence and policy worlds.

For example, one objective of the plan is to communicate more regularly and systematically with interested groups and individuals — including the Canadian intelligence community, organizations that deal with intelligence issues, and academics specializing in the intelligence field — about the nature of my mandate, my approach to the job, and the activities of my office. This type of interaction could lead, for instance, to productive partnerships with academic specialists in areas of mutual interest and concern. In addition, conveying accurate,

---

timely information about the office will help avoid misunderstandings or speculation about who we are and what we do.

Among the first steps in implementing the plan were my meetings with the current and former Ministers of National Defence, the chair and members of the Security Intelligence Review Committee, and the National Security Adviser to the Prime Minister, mentioned earlier.

In addition, my staff met with academics specialized in security and intelligence matters and participated in meetings of the Canadian Association of Security and Intelligence Studies. My staff also took steps toward greater participation in the public service community — notably through meetings with other small agencies, particularly those whose mandates include reviews and complaints.

With regard to the broader security and intelligence community, my office received visiting parliamentarians from Sweden and the United Kingdom — both countries with similar concerns but different review models from Canada's. In the past the office would not have had sufficient staff resources to undertake this range of activities, but the hiring of a director of review and government liaison and a director of review and military liaison will permit continued involvement in these communities in the future.

## LOOKING AHEAD

### New national security policy

On April 27, 2004, the government tabled in Parliament its first national security policy, entitled *Securing an Open Society: Canada's National Security Policy*. The policy addresses a range of national security issues and provides guidance in six strategic areas: intelligence, emergency planning and management, public health, transport security, border security, and international security.



The policy also calls for the development of new structures and strategies that the government believes will enable it to anticipate and manage current and future threats to Canada's national security interests.

Among the changes in government structure announced on December 12, 2003, and confirmed in the national security policy announcement, was a proposal to establish a new committee of parliamentarians whose members would be sworn in as Privy Councillors so they could be briefed on national security issues.

These initiatives obviously have the potential to influence the activities of my office, but it is too early to say what the shape or extent of this influence might be. My staff and I will be following developments closely with a view to providing input where appropriate.

## Proposed legislation

Two legislative proposals before Parliament at the end of this reporting year may have additional implications for my office:

- Passage of Bill C-7 (formerly Bill C-17), the Public Safety Act, 2002, would entail new responsibilities for the Commissioner. The bill amends the *National Defence Act* to confer significant new responsibilities on the Commissioner of CSE for reviewing the lawfulness of activities undertaken by the Department of National Defence and the Canadian Forces to maintain and protect their computer systems and networks and for dealing with complaints arising from such activities.<sup>6</sup>

---

<sup>6</sup> Bill C-7, An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order to enhance public safety, 3rd Sess., 37th Parl., 2004; Bill C-17, An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order to enhance public safety, 2nd Sess., 37th Parl., 2002.

- Bill C-14 (formerly Bill C-32) amends provisions of the *Criminal Code* and the *Financial Administration Act*, among other acts. It introduces new provisions, including a new authority to intercept private communications for the purpose of managing and protecting computer systems and networks. There is a question of how this bill will affect the provisions and passage of the proposed Public Safety Act, 2002, which has similar wording.<sup>7</sup>

My concerns are threefold:

- the fact that passage of both bills would establish different governing authorities dealing with essentially similar activities;
- the fact that passage of Bill C-7 would impose on the Department of National Defence a different accountability regime than would be imposed on other departments by passage of Bill C-14; and
- the difficulties I am likely to encounter in providing meaningful assurance of lawfulness and compliance with ministerial authority as envisaged in Bill C-7.

Developments in two other areas may also have implications for my office:

- Parliament's statutory review of the *Anti-Terrorism Act* three years after its initial passage into law is slated to begin by the end of 2004. I intend to provide my comments based on my observations to date.
- The government introduced Bill C-25, the so-called whistle-blower legislation, on

---

<sup>7</sup> Bill C-14, An Act to amend the *Criminal Code* and other Acts, 3rd Sess., 37th Parl., 2004; Bill C-32, An Act to amend the *Criminal Code* and other Acts, 2nd Sess., 37th Parl., 2003.

March 22, 2004.<sup>8</sup> Although CSE would be exempt from this legislation, it would have to establish a system to serve essentially the same purpose, raising questions about a possible role for the Commissioner.

We will be following these and other developments closely to determine their likely impact on this office, as well as where and how we can contribute our input most effectively.

## Review agencies conference

The next International Intelligence Review Agencies Conference will be held in Washington, D.C., in October 2004. Representatives of review agencies from Australia, Canada, New Zealand, the United States, the United Kingdom and other countries will meet to exchange views on issues of common interest. I look forward to receiving this year's agenda.

## CONCLUDING THOUGHTS

Looking back over the year, I would like to thank my predecessor as Commissioner, the Honourable Claude Bisson, O.C., who laid a strong foundation for the Office of the CSE Commissioner and from whom I inherited a superb staff and an organization well positioned to meet the challenges ahead. Thanks to this legacy, the transition between our tenures was smooth, and I was able to assume my responsibilities quickly and efficiently.

Based on my experience over the past nine months, I believe that my mandate and resources as Commissioner are adequate to discharge my legislated duties. I look forward to continuing the productive relationship established with the Minister, with CSE and with other government officials as we fulfil our respective roles in Canada's security and intelligence community.

---

<sup>8</sup> An Act to establish a procedure for the disclosure of wrongdoings in the public sector, including the protection of persons who disclose the wrongdoings. Its short title would be the Public Servants Disclosure Protection Act, 3rd Sess., 37th Parl., 2004.



---

# Mandate of the Communications Security Establishment Commissioner

## *National Defence Act – Part V.1*

“**273.63** (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

**“273.65** (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.”

*Security of Information Act*

**“15.** (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest.

**“15.** (5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following:

**“15.** (5) (b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person’s possession to,

(ii) the Communications Security Establishment Commissioner, if the person’s concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person’s duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.”

---

## Statement of Expenditures 2003-2004

### Standard Object Summary

Salaries and Wages	352,505
Transportation and Telecommunications	22,227
Information	43,201
Professional and Special Services	246,323
Rentals	134,794
Purchased Repair and Maintenance	42,019
Materials and Supplies	9,708
Acquisition of Machinery and Equipment	51,451
Other Expenditures	104
<b>Total</b>	<b>\$902,332</b>





---

## Classified Reports, 1996-2004

Classified Report to the Minister – March 3, 1997 (TOP SECRET)

Classified Report to the Minister

- Operational Policies with Lawfulness Implications - February 6, 1998 - (SECRET)

Classified Report to the Minister

- CSE's Activities under \*\*\* - March 5, 1998 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- Internal Investigations and Complaints - March 10, 1998 (SECRET)

Classified Report to the Minister

- CSE's activities under \*\*\* - December 10, 1998 (TOP SECRET/CEO)

Classified Report to the Minister

- On controlling communications security (COMSEC) material - May 6, 1999 (TOP SECRET)

Classified Report to the Minister

- How We Test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) - June 14, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- A Study of the \*\*\* Collection Program - November 19, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- On \*\*\* - December 8, 1999 (TOP SECRET - COMINT)

Classified Report to the Minister

- A Study of the \*\*\* Reporting Process - an overview (Phase I) - December 8, 1999 (SECRET/CEO)

Classified Report to the Minister

- A Study of Selection and \*\*\* - an overview - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's Operational Support Activities Under \*\*\* - follow-up - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- Internal Investigations and Complaints - follow-up - May 10, 2000 (SECRET)

Classified Report to the Minister

- On findings of an external review of CSE's ITS Program - June 15, 2000 (SECRET)

Classified Report to the Minister

- CSE's Policy System Review - September 14, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- A study of the \*\*\* Reporting Process - Phase II \*\*\* - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister

- A study of the \*\*\* Reporting Process - Phase III \*\*\* - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister

- CSE's participation \*\*\* - August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's support to \*\*\* as authorized by \*\*\* and \*\*\* - August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister

- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) - August 21, 2002 (SECRET)

Classified Report to the Minister

- CSE's support to XXX, as authorized by \*\*\* and code named \*\*\* - November 13, 2002 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's SIGINT activities carried out under the \*\*\* 2002 \*\*\* ministerial authorization November 27, 2002 (TOP SECRET/CEO)

Classified Report to the Minister

- Lexicon - 26 March 2003 (TOP SECRET/COMINT)

Classified Report to the Minister

- CSE's activities pursuant to three XXX ministerial authorizations including \*\*\* - May 20, 2003 (SECRET)

Classified Report to the Minister

- CSE's support to XXX, as authorized by \*\*\* and code named \*\*\* - Part I - November 6, 2003 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister

- CSE's support to XXX, as authorized by \*\*\* and code named \*\*\* - Part II - March 15, 2004 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister

- A review of CSE's activities conducted under XXX ministerial authorization - March 19, 2004 (SECRET/CEO)

Classified Report to the Minister

- Internal investigations and complaints - Follow-up - March 25, 2004 (TOP SECRET/CEO)



Classified Report to the Minister  
- Lexicon - 26 mars 2003 (TRÈS SECRET/COMINT)

Classified Report to the Minister  
- CSE's activities pursuant to three XXX ministerial authorizations including  
\*\*\*\* - 20 mai 2003 (SECRET)

Classified Report to the Minister  
- CSE's support to XXX, as authorized by \*\*\* and code named \*\*\* - Part I - N  
6 novembre 2003 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

Classified Report to the Minister  
- CSE's support to XXX, as authorized by \*\*\* and code named \*\*\* - Part II -  
15 mars 2004 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

Classified Report to the Minister  
- A review of CSE's activities conducted under XXX ministerial authorization -  
19 mars 2004 (SECRET/Réserve aux canadiens)

Classified Report to the Minister  
- Internal investigations and complaints - Follow-up - 25 mars 2004  
(TRÈS SECRET/Réserve aux Canadiens)

- Classified Report to the Minister
- CSE's Operational Support Activities Under \*\*\* - follow-up - 10 mai 2000 (TRÈS SECRET/Réserve aux Canadiens)
- Classified Report to the Minister
- Internal Investigations and Complaints - follow-up - 10 mai 2000 (SECRET)
- Classified Report to the Minister
- On findings of an external review of CSE's ITS Program - 15 juin 2000 (SECRET)
- Classified Report to the Minister
- CSE's Policy System Review - 14 septembre 2000 (TRÈS SECRET/Réserve aux Canadiens)
- Classified Report to the Minister
- A study of the \*\*\* Reporting Process - Phase II \*\*\* - 6 avril 2001 (SECRET/Réserve aux Canadiens)
- Classified Report to the Minister
- A study of the \*\*\* Reporting Process - Phase III \*\*\* - 6 avril 2001 (SECRET/Réserve aux Canadiens)
- Classified Report to the Minister
- CSE's participation \*\*\* - 20 août 2001 (TRÈS SECRET/Réserve aux Canadiens)
- Classified Report to the Minister
- CSE's support to \*\*\*, as authorized by \*\*\* and \*\*\* - 20 août 2001 (TRÈS SECRET/Réserve aux Canadiens)
- Classified Report to the Minister
- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) - 20 août 2002 (SECRET)
- Classified Report to the Minister
- CSE's support to XXX as authorized by \*\*\* and code named \*\*\* - 13 novembre 2002 (TRÈS SECRET/Réserve aux Canadiens)
- Classified Report to the Minister
- CSE's SIGINT activities carried out under the \*\*\* 2002 \*\*\* ministerial authorization - 27 novembre 2002 (TRÈS SECRET/Réserve aux Canadiens)

## Rapports classifiés de 1996 à 2004

Classified Report to the Minister - 3 mars 1997 (TRÈS SECRET)

Classified Report to the Minister  
- Operational Policies with Lawfulness Implications - 6 février 1998 - (SECRET)

Classified Report to the Minister  
- CSE's activities under \*\*\* - 5 mars 1998 (TRÈS SECRET Mot codé/Réserve aux Canadiens)

Classified Report to the Minister  
- CSE's activities under \*\*\* - 10 décembre 1998 (TRÈS SECRET/Réserve aux Canadiens)

Classified Report to the Minister  
- On controlling communications security (COMSEC) material - 6 mai 1999 (TRÈS SECRET)

Classified Report to the Minister  
- How We Test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) - 14 juin 1999 (TRÈS SECRET Mot codé/Réserve aux Canadiens)

Classified Report to the Minister  
- A Study of the \*\*\* Collection Program - 19 novembre 1999 (TRÈS SECRET Mot codé/Réserve aux Canadiens)

Classified Report to the Minister  
- On \*\*\* - 8 décembre 1999 (TRÈS SECRET - COMINT)

Classified Report to the Minister  
- A Study of the \*\*\* Reporting Process - an overview (Phase I) - 8 décembre 1999 (SECRET/Réserve aux Canadiens)

Classified Report to the Minister  
- A Study of Selection and \*\*\* - an overview - 10 mai 2000 (TRÈS SECRET/Réserve aux Canadiens)





Sommaire des articles courants	
Traitements et salaires	352 505
Transports et télécommunications	22 227
Information	43 201
Services professionnels et spéciaux	246 323
Location	134 794
Achat de services de réparation et d'entretien	42 019
Fournitures et approvisionnements	9 708
Acquisition de machines et de matériel	51 451
Autres charges	104
<b>Total</b>	<b>902 332 \$</b>

« 273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre. »

*Loi sur la protection de l'information*

« 15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public.

« 15. (5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes :

« 15. (5) (b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession :

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable. »

## Mandat du commissaire du Centre de la sécurité des télécommunications

*Loi sur la défense nationale - Partie V.1*

« 273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

(a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

(b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

(c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

La prochaine conférence internationale des organismes d'examen des activités de renseignement se tiendra à Washington (D.C.), en octobre 2004. Des représentants des organismes d'examen de l'Australie, du Canada, de la Nouvelle-Zélande, des États-Unis, du Royaume-Uni et d'autres pays se réuniront alors pour échanger des vues sur des questions d'intérêt commun. J'attends de recevoir l'ordre du jour de cette année.

Au moment de conclure cette rétrospective, je tiens à remercier mon prédécesseur, l'honorable Claude Bisson, O.C., qui a solidement établi le bureau du commissaire du CST et m'a légué un personnel magnifique et une organisation bien placée pour relever les défis de l'avenir. Grâce à cela, la transition entre son administration et la mienne s'est faite sans heurt, et j'ai pu assumer mes responsabilités rapidement et efficacement.

En me fondant sur mon expérience des neuf derniers mois, j'estime que mon mandat et les ressources mises à ma disposition sont suffisants pour me permettre de m'acquitter des fonctions que me confère la loi. Je compte entretenir les relations productives établies avec le ministre, avec le CST et avec d'autres fonctionnaires tandis que nous remplirons nos rôles respectifs au sein de la collectivité canadienne du renseignement et de la sécurité.



J'ai trois préoccupations à ce sujet, soit :

- le fait que l'adoption des deux projets de loi établirait des autorisations différentes pour régir des activités essentiellement semblables;
- le fait que l'adoption du projet de loi C-7 imposerait au ministère de la Défense nationale un régime de responsabilisation différent de celui que l'adoption du projet de loi C-14 imposerait aux autres ministères;
- les difficultés auxquelles je me heurterai probablement lorsqu'il s'agira de donner la garantie sérieuse de légalité et de conformité à l'autorisation ministérielle prévue par le projet de loi C-7.

Des faits nouveaux se rattachant à deux autres domaines pourraient également avoir des incidences sur mon bureau :

- l'examen réglementaire de la *Loi antiterroriste* de 2004. J'entends apporter mes commentaires en me fondant sur les observations que j'ai faites jusqu'ici;

- le 22 mars 2004, le gouvernement a déposé le projet de loi C-25, ou mesure législative sur la dénonciation<sup>8</sup>. Le CST serait soustrait à cette mesure législative, mais il devrait néanmoins établir un système qui servirait essentiellement à la même fin, ce qui soulève des questions sur un rôle éventuel du commissaire.

Nous suivrons de près ces faits nouveaux et d'autres afin de déterminer leur incidence probable sur mon bureau, ainsi que les domaines où notre apport peut être le plus utile et la façon la plus efficace de le fournir.

<sup>8</sup> Loi prévoyant un mécanisme de dénonciation des actes répréhensibles dans le secteur public et de protection des dénonciateurs. Son titre abrégé serait : *Loi sur la protection des fonctionnaires dénonciateurs d'actes répréhensibles*, 3<sup>e</sup> sess., 37<sup>e</sup> Parl., 2004.

## Mesures législatives proposées

influence. Mon personnel et moi-même suivrons les événements de près dans le but d'apporter un appoint lorsque ce sera à propos.

Deux projets de loi à l'étude au Parlement à la fin de l'année sur laquelle porte le présent rapport pourraient avoir d'autres incidences sur mon bureau :

- le projet de loi C-7 (auparavant projet de loi C-17) est une mesure législative d'ensemble intitulée Loi de 2002 sur la sécurité publique, dont l'adoption entraînerait de nouvelles responsabilités pour le commissaire. Ce projet de loi modifierait la *Loi sur la défense nationale* de manière à attribuer au commissaire du CST de nouvelles responsabilités importantes touchant l'examen de la légalité des mesures prises par le ministère de la Défense nationale et par les Forces canadiennes pour entretenir et protéger leurs systèmes et réseaux informatiques et pour traiter les plaintes découlant de ces mesures<sup>6</sup>;
- le projet de loi C-14 (auparavant projet de loi C-32) modifie, entre autres, des dispositions du *Code criminel* et de la Loi sur la gestion des finances publiques. Il instaure de nouvelles dispositions, dont un nouveau pouvoir d'intercepter des communications privées afin de gérer et de protéger les systèmes et réseaux informatiques. On se demande quels effets ce projet de loi aura sur les dispositions et l'adoption du projet de Loi de 2002 sur la sécurité publique, dont le libellé est semblable<sup>7</sup>.

<sup>6</sup> Projet de loi C-7, *Loi modifiant certaines lois fédérales et édictant des mesures de mise en œuvre de la convention sur les armes biologiques ou à toxines, en vue de renforcer la sécurité publique*, 3<sup>e</sup> sess., 37<sup>e</sup> Parl., 2004; projet de loi C-17, *Loi modifiant certaines lois fédérales et édictant des mesures de mise en œuvre de la convention sur les armes biologiques ou à toxines, en vue de renforcer la sécurité publique*, 2<sup>e</sup> sess., 37<sup>e</sup> Parl., 2002. <sup>7</sup> Projet de loi C-14, *Loi modifiant le Code criminel et d'autres lois*, 3<sup>e</sup> sess., 37<sup>e</sup> Parl., 2004; projet de loi C-32, *Loi modifiant le Code criminel et d'autres lois*, 2<sup>e</sup> sess., 37<sup>e</sup> Parl., 2003.

# COUP D'ŒIL SUR L'AVENIR La nouvelle politique de sécurité nationale

En ce qui concerne la collectivité plus générale de la sécurité et du renseignement, mon bureau a reçu la visite de parlementaires de la Suède et du Royaume-Uni, deux pays qui ont des préoccupations similaires à celles du Canada, mais des modèles d'examen différents. Par le passé, le bureau ne disposait pas d'un personnel suffisant pour se livrer à toutes ces activités, mais le recrutement d'un directeur de l'examen et de la liaison gouvernementale et d'un directeur de l'examen et de la liaison militaire permettra de poursuivre les relations avec ces collectivités à l'avenir.

Le 27 avril 2004, le gouvernement a déposé au Parlement sa première politique de sécurité nationale, intitulée *Protéger une société ouverte : la politique canadienne de sécurité nationale*. Celle-ci aborde un grand nombre de questions de sécurité nationale et fournit une orientation dans six domaines stratégiques, soit : le renseignement, la planification et la gestion des opérations d'urgence, la santé publique, la sécurité des transports, la sécurité des frontières, et la sécurité internationale. Elle prévoit en outre l'élaboration de nouvelles structures et stratégies qui, de l'avis du gouvernement, lui permettront de prévoir et de gérer les menaces actuelles et futures pour les intérêts nationaux du Canada en matière de sécurité.

Parmi les modifications de la structure du gouvernement annoncées le 12 décembre 2003 et confirmées lors de l'annonce de la politique de sécurité nationale figurait une proposition visant la constitution d'un nouveau comité de parlementaires dont les membres seraient assermentés à titre de conseillers privés pour recevoir des séances d'information sur les questions de sécurité nationale. Ces initiatives pourraient manifestement influer sur les activités de mon bureau, mais il est trop tôt pour prédire la nature ou l'étendue éventuelles de cette

concours d'acteurs clés de la collectivité canadienne du renseignement aidera à guider mon bureau dans les univers en évolution rapide du renseignement et des politiques.

Par exemple, l'un des objectifs du plan consiste à entretenir des communications plus régulières et plus systématiques avec les groupes et particuliers intéressés — notamment la collectivité canadienne du renseignement, les organismes qui traitent des questions de renseignement et les universitaires spécialisés dans le domaine du renseignement — au sujet de la nature de mon mandat, de ma façon d'aborder mon travail et des activités de mon bureau. Ce genre d'interaction pourrait mener, par exemple, à des partenariats productifs avec des spécialistes des universités dans des domaines d'intérêt et de préoccupation mutuels. De plus, la communication de renseignements exacts et opportuns au sujet de mon bureau aidera à éviter les malentendus ou les conjectures au sujet de sa nature et de ses activités.

Mes rencontres avec le ministre de la Défense nationale actuel et son prédécesseur, avec le président et les membres du Comité de surveillance des activités de renseignement de sécurité et avec le conseiller en matière de sécurité nationale auprès du Premier ministre, dont je fais mention plus haut, ont été parmi les premières mesures d'exécution de ce plan.

De plus, des membres de mon personnel ont rencontré des universitaires spécialisés en matière de sécurité et de renseignement et participé aux réunions de l'Association canadienne pour l'étude de la sécurité et du renseignement. Ils ont également pris des initiatives en vue de participer davantage à la collectivité de la fonction publique, notamment en rencontrant des représentants d'autres petits organismes, en particulier ceux dont le mandat comporte des examens et l'étude de plaintes.



Comme les rapports annuels précédents en traitent dans le détail et le présent rapport en fait mention plus haut, deux caractéristiques de la *Loi antiterroriste* de décembre 2001 ont influé directement sur les fonctions du commissaire, soit l'examen des activités entreprises par le CST en vertu d'une autorisation ministérielle, et les fonctions assignées au commissaire en vertu de la *Loi sur la protection de l'information*.

Pour lui permettre de s'acquitter de ces nouvelles responsabilités, on a alloué des ressources additionnelles à mon bureau en vue de l'exécution des travaux d'examen. L'accroissement de la charge de travail et du personnel a influé sur notre façon d'organiser et de gérer notre travail. Par exemple, nous avons amélioré nos politiques et procédures internes de gestion du bureau pour tenir compte du développement de l'organisation et de l'augmentation du personnel au cours de l'année financière.

Nous nous sommes en outre penchés sur nos méthodes de travail. Des outils comme une méthodologie normalisée, des énoncés de portée et des lignes directrices structurent nos examens des activités du CST de sorte que les examinateurs travaillent avec la même rigueur et la même minutie. Comme un plus grand nombre de personnes participent à ces efforts, mon bureau a entrepris de consigner et de décrire ces processus dans tous les cas où c'est possible.

Vu ma nouvelle nomination et l'évolution du mandat du commissaire au cours des trois dernières années, le moment était venu d'examiner les rapports qu'entretenait mon bureau dans le contexte plus général où il exerce son activité, notamment avec la collectivité du gouvernement fédéral et la collectivité de la sécurité et du renseignement au Canada et à l'échelle internationale. Un plan de communication élaboré cette année avec le

## LE BUREAU DU COMMISSAIRE Dépenses du bureau et personnel

<sup>5</sup> L.R.C. (1985), chap. O-5.

Personne ne s'est adressé à moi pour se prévaloir des dispositions relatives à la défense d'intérêt public qui figurent au sous-alinéa 15(5)b)(ii) de la *Loi sur la protection de l'information*<sup>5</sup>.

Toutes les plaintes qui me sont présentées au sujet des activités du CST doivent par conséquent être examinées dans cette optique.

V.1 de la *LDN* (voir note 4).

Si je dois être en mesure d'assurer aux plaignants que le CST ne se livre pas à des activités illégales, je dois aborder les plaintes en tenant compte du mandat assigné au CST par la partie V.1 de la *Loi sur la défense nationale*. À l'heure actuelle, tout comme avant l'instauration de la partie V.1, le CST ne doit pas cibler les communications de Canadiens ni de personnes se trouvant au Canada. Or, comme je le mentionne plus haut, il n'est désormais plus possible d'affirmer sans équivoque que les deux pôles d'une communication interceptée par le CST sont étrangers. Le CST peut maintenant intercepter (mais non cibler) des communications privées à condition d'obtenir à l'avance une autorisation ministérielle. Il peut aussi utiliser et conserver ces communications à condition de respecter les lignes directrices qui sont également énoncées à la partie V.1 de la *LDN* (voir note 4).

Depuis la création de son poste, en 1996, le mandat du commissaire du Centre de la sécurité des télécommunications et, par conséquent, le personnel et les autres ressources nécessaires à l'exécution de ce mandat ont considérablement évolué. Entre juin 1996 et décembre 2001, le commissaire avait pour rôle d'examiner les activités du CST pour déterminer si elles étaient conformes à la loi, et de recevoir les plaintes relatives à la légalité de ces activités.

## Constatations faites en 2003-2004

Comme je le dis clairement dans ce rapport, mes recommandations et celles de mon prédécesseur visent généralement à prévenir la possibilité de non-conformité par la mise en place de mécanismes de contrôle efficaces. C'est dans cet esprit que je continuerai à vérifier la suite donnée par le CST aux recommandations de mon bureau.

Je puis déclarer que les activités du CST que mon bureau a examinées au cours de la dernière année étaient conformes à la loi et à l'autorisation ministérielle. Il importe de situer cette affirmation dans son contexte. Elle ne signifie pas que je certifie que toutes les activités exercées par le CST en 2003-2004 étaient légales. Je ne peux affirmer cela, car je n'ai pas examiné toutes ses activités — et aucun examinateur indépendant ne pourrait le faire. Toutefois, mon bureau examine un grand nombre d'activités en profondeur, en fonction de notre évaluation des domaines où les risques d'activité illégale sont les plus grands. Tel est le contexte dans lequel il faut envisager la garantie que fournit mon travail.

Je me dois cependant d'ajouter que, au cours des examens, je décèle parfois des circonstances où il existe des risques manifestes d'activité illégale possible (par exemple, en raison de faiblesses dans les politiques ou les pratiques). Tout comme mon prédécesseur, j'ai pour règle de signaler ces circonstances au CST et au ministre. Comme je le déclare clairement dans l'introduction de ce rapport, j'estime qu'il est plus utile de prévenir les activités illégales que de les déceler après le fait.

## Plaintes et préoccupations au sujet des activités du CST

Deux plaintes ont été formulées pendant la période couverte par ce rapport, mais ni l'une ni l'autre n'a entraîné une enquête officielle.

## Examen des recommandations antérieures

Certaines faiblesses inhérentes aux politiques et aux procédures relatives à ces activités ont été portées à l'attention du CST. Certaines questions ont été résolues, mais d'autres subsistent. J'espère pouvoir traiter de celles-ci dans mon rapport de l'année prochaine.

On trouvera à l'annexe C la liste de tous les rapports classifiés adressés au ministre par mon prédécesseur et par moi-même depuis l'établissement du bureau du commissaire, en 1996.

Cette année, mon personnel a passé en revue toutes les recommandations faites par mon prédécesseur et par moi-même dans des rapports classifiés présentés au ministre de la Défense nationale depuis la création de mon bureau, en 1996. Ce travail avait pour but de vérifier la suite donnée à ces recommandations par le CST et de déterminer si les problèmes relevés avaient été réglés de façon satisfaisante. Je demanderai au CST de faire le point annuellement à ce sujet.

Cet examen a révélé que la réponse du CST aux recommandations n'avait pas été uniforme. Cela n'est pas étonnant, compte tenu de la diversité de celles-ci : certaines pouvaient être mises en œuvre immédiatement; certaines avaient trait à la politique ou aux procédures; d'autres étaient de caractère technique, et d'autres encore nécessitaient une étude plus poussée destinée à déterminer leur faisabilité. Beaucoup se rapportaient à la façon dont le CST pourrait mieux gérer ses activités et en rendre compte.

En me fondant sur cet examen, je ferais remarquer que le CST a répondu à beaucoup des recommandations du commissaire, mais qu'il lui reste un certain nombre de questions à aborder, en particulier en établissant des plans de travail et des échéanciers assortis d'étapes et de dates d'achèvement pour les mesures correctives dont il a reconnu la nécessité.



J'ai adressé cinq rapports classifiés au ministre de la Défense nationale au cours de la période couverte par le présent rapport. Deux de ceux-ci avaient été entrepris par mon prédécesseur et ont été achevés pendant la première année de mon mandat.

En 2003-2004, j'ai présenté au ministre de la Défense nationale trois rapports classifiés portant sur des sujets liés à mon mandat général d'examiner les activités du CST pour assurer leur conformité à la loi. La présentation d'un rapport classifié au ministre ne signifie pas qu'un défaut de conformité à la loi ou à l'autorisation ministérielle a été détecté. Elle indique seulement que le rapport contient des éléments qui exigent une classification. Je fais rapport au ministre de tous mes examens, soit pour le rassurer, soit pour lui signaler des préoccupations, selon ce que la situation exige.

Le CST a entrepris des activités en vertu de sept autorisations ministérielles en 2002-2003; sur celles-ci, deux concernaient la collecte de renseignements étrangers et cinq avaient trait à la sécurité des technologies de l'information. Au cours de la période couverte par le présent rapport, mon bureau a examiné les activités menées en vertu de cinq des AM; l'examen des autres activités était presque terminé à la fin de l'année faisant l'objet du rapport. Les cinq examens ont débouché sur la présentation de deux rapports au ministre, portant tous les deux sur les activités relatives à la sécurité des technologies de l'information.

Aucun de ces rapports n'a soulevé de questions d'illegalité. Toutefois, une question plus générale au sujet de la structure des autorisations ministérielles et de leur processus d'utilisation s'est posée.

Le rapport de la vérificatrice générale daté de novembre 2003 a été déposé au Parlement le 11 février 2004. Le chapitre 10 de ce rapport — Autres observations de vérification — comprenait une note de vérification intitulée *Les activités de surveillance indépendante visant les organismes de sécurité et de renseignement*, qui disait ceci : « Il y a manque de cohérence quant au degré de surveillance et aux obligations de divulgation auxquels les organismes de sécurité et de renseignement sont soumis. »

La vérificatrice générale donnait à entendre que le rapport annuel du commissaire du CST devrait traiter, en plus de la conformité du CST à la loi, de sujets comme les questions de gestion ou les problèmes potentiels au CST. Je pense qu'un examen des rapports annuels publiés par mon bureau jusqu'ici révélera que ces sujets ont effectivement été abordés, car ils ont trait à deux des secteurs d'activité de l'organisme, soit la collecte de renseignements étrangers et la protection des systèmes et réseaux d'information du gouvernement.

Par exemple, ces dernières années, les examens ont mené à la formulation d'observations dans des domaines comme les activités de planification stratégique du CST, ses politiques, procédures et pratiques internes, et les cadres de gestion et de contrôle. Ces observations ont cependant toujours été faites dans le contexte de la légalité et des efforts déployés par le CST pour sauvegarder la vie privée des Canadiens.

Je pense que la teneur du rapport annuel public du commissaire du CST doit être déterminée par son mandat, qui est d'examiner les activités du CST et d'en faire rapport du point de vue de leur conformité à la loi, et de faire rapport annuellement au ministre de la Défense nationale de ses propres activités et de ses constatations.

Les technologies intégrées d'aujourd'hui écoulent différents genres de trafic et suivent des voies de communication complexes qui traversent les frontières internationales et mêlent les communications étrangères avec les communications privées. Les dispositions relatives à l'AM ne permettent pas au CST de cibler les Canadiens ni leurs communications. (Le CST n'a jamais été autorisé à faire cela.) Aujourd'hui, le CST est cependant mieux à même de s'acquitter de ses responsabilités en matière de renseignement étranger parce qu'il peut, avec le consentement du ministre, cibler les communications étrangères même si elles ont un lien avec le Canada. Je pense que peu de Canadiens se trouveraient en désaccord avec l'objet de cette disposition et le pouvoir qu'elle donne dans le contexte actuel de terrorisme et de menaces pour la sûreté et la sécurité des Canadiens.

Je suis à même d'affirmer que, depuis l'adoption de cette nouvelle mesure législative, le CST a exercé ce pouvoir. À titre de commissaire du CST, j'en comprends le besoin et j'en appuie l'objectif. Le paragraphe 273.65(8) de la *LDN* m'oblige à examiner les activités exercées par le CST en vertu d'une AM pour m'assurer qu'elles sont autorisées, et à faire rapport annuellement au ministre.

Je pense que les politiques, instruments et processus du CST doivent exiger et faciliter la gestion et la responsabilisation de toutes les activités qu'il exerce en vertu d'une AM, en particulier celles qui ont trait à l'interception de communications privées et à la sauvegarde de la vie privée des Canadiens. Bien que ce processus évolue, je peux déclarer que le CST a continué d'améliorer la structure de l'AM et en a renforcé les mécanismes de gestion et de responsabilisation.

nationaux et de déceler et contre les menaces planant sur ceux-ci. L'avènement de technologies nouvelles ainsi que les progrès révolutionnaires accomplis dans l'industrie des communications au cours de la dernière décennie ont entravé certaines formes traditionnelles de collecte de renseignements, dont celle du renseignement électromagnétique étranger effectuée par le CST.

Il n'y a pas si longtemps, la collecte de renseignements étrangers s'articulait autour de modes et de technologies de communication prévisibles. Elle pouvait par conséquent être effectuée à l'intérieur de cadres juridiques relativement bien définis. Ce contexte facilitait l'examen et l'évaluation des activités de collecte de ces renseignements. Au cours de la première année de mon mandat de commissaire du CST, toutefois, j'ai vite compris que ce n'est plus le cas. Les gouvernements ont dû réévaluer leur capacité de protéger les intérêts nationaux et de contre des activités comme le terrorisme, qui menacent la sécurité nationale et internationale. Le Canada ne fait pas exception à cet égard.

De nouveaux mécanismes juridiques étaient nécessaires pour tenir compte de ce contexte en mutation. Les dispositions relatives à l'autorisation ministérielle (AM), ajoutées à la partie V.1 de la *Loi sur la défense nationale* en 2001, ont constitué l'une de ces réponses <sup>4</sup>.

<sup>4</sup> La partie V.1 a été ajoutée à la *Loi sur la défense nationale* par la *Loi antiterroriste*, qui est entrée en vigueur le 24 décembre 2001. Avant de donner une autorisation, le ministre doit être convaincu que les quatre conditions énoncées au paragraphe 273.65(2) de la *LDN* sont remplies, soit :

- a) l'interception vise des entités étrangères situées à l'extérieur du Canada;
- b) les renseignements à obtenir ne peuvent raisonnablement être obtenus d'une autre manière;
- c) la valeur des renseignements étrangers que l'on espère obtenir grâce à l'interception justifie l'interception envisagée;
- d) il existe des mesures satisfaisantes pour protéger la vie privée des Canadiens et pour faire en sorte que les communications privées ne seront utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité.



Ce qui est nouveau, c'est le pouvoir que lui confère la LBN d'intercepter des communications privées, dans des conditions prescrites, s'il est autorisé à cette fin par le ministre de la Défense nationale<sup>3</sup>. Lorsqu'il possède une autorisation ministérielle, le CST peut intercepter et utiliser une communication ayant un rapport avec le Canada (c'est-à-dire une « communication privée ») acquise à l'occasion du ciblage d'une entité étrangère à l'étranger, pourvu qu'il satisfasse à certaines conditions énoncées dans la LBN. Cette disposition ajoute un nouveau pouvoir au cadre juridique à l'intérieur duquel les renseignements étrangers peuvent être acquis légalement.

À la suite de mon examen initial de certaines activités de collecte de renseignements étrangers, je me suis inquiété de ce que, dans certains cas, l'on ne tenait pas dûment compte des liens entre ces activités et les autorisations qui les régissent. J'ai donc été heureux d'apprendre que, au cours de la dernière année, on avait réexaminé les cadres juridiques mis à la disposition de la collectivité du renseignement aux fins de la collecte de renseignements étrangers, afin d'assurer que l'on avait pleinement tenu compte de toutes les autorisations disponibles avant d'autoriser les activités de renseignements étrangers. J'encourage le gouvernement à continuer d'agir dans ce sens.

Par le passé, les gouvernements compilaient sur la collecte de renseignements dans le cadre de leurs efforts en vue de protéger et promouvoir les intérêts

## Autorisations ministérielles

<sup>3</sup> Les *communications privées* sont les communications de Canadiens ou de personnes se trouvant au Canada. Plus précisément, l'article 183 du *Code criminel* définit une *communication privée* comme suit : communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.

## Autorisations régissant la collecte de renseignements étrangers

À la lumière de ces faits, plusieurs questions générales liées à la collecte de renseignements étrangers ont attiré mon attention au cours de la dernière année; deux d'entre elles méritent d'être examinées ici.

Les besoins de renseignement du Canada, y compris ses priorités en matière de renseignements étrangers, sont établis annuellement par le Comité spécial sur les priorités en matière de renseignement (auparavant la Réunion des ministres sur la sécurité et le renseignement), que préside le Premier ministre. Plusieurs organismes fédéraux, dont le Centre de la sécurité des télécommunications, contribuent à répondre à ces priorités.

Pour remplir son mandat en matière de renseignements étrangers, le CST s'appuie sur la *Loi sur la défense nationale* (*LDN*<sup>2</sup>), qui l'habilite à « acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement ». Lorsque il fait cela, le CST agit à titre de fournisseur *principal* de renseignements étrangers.

En vertu de la *LDN*, le CST aide en outre d'autres organismes fédéraux à remplir les fonctions que leur confère la loi. Dans ces cas, il fait fonction d'*agent*. Lorsqu'il apporte une aide technique et opérationnelle aux organismes fédéraux d'exécution de la loi et de sécurité, le CST est régi strictement par les modalités des autorisations régissant l'organisme principal, qui, dans certains cas, peuvent être un mandat de la Cour fédérale du Canada.

Ces deux rôles — celui de fournisseur principal et celui d'*agent* — ont été officialisés dans la loi en 2001, mais ils ne sont pas nouveaux pour le CST.

<sup>2</sup> L.R.C. (1985), chap. N-5.

J'ai vite pris conscience de l'ensemble des défis auxquels sont confrontés le CST et le reste de la collectivité du renseignement compte tenu des menaces mondialisées qui ont des incidences sur les affaires internationales, sur la défense et sur la sécurité du Canada. Il est capital de surveiller ces menaces et de les comprendre; néanmoins, les efforts déployés dans ce sens ont été restreints ces dernières années par ce qui est devenu un réseau de plus en plus complexe de technologies de communication mondiale. Ce contexte présente en outre des défis importants pour ce qui est de la collecte de renseignements étrangers, qui constitue l'un des principaux mandats du CST<sup>1</sup>.

Ces défis et d'autres exigences nouvelles ont entraîné des modifications législatives et l'élaboration de nouveaux cadres juridiques qui devraient favoriser l'atteinte de deux objectifs, soit faciliter les activités des organismes de renseignement, et exiger que ceux-ci satisfassent à certaines normes et respectent certains seuils qui leur permettent de définir leurs activités et d'en rendre compte.

Parallèlement à l'évolution technologique visant à permettre la collecte de renseignements étrangers dans un contexte de communications mondiales de plus en plus large et complexe, il importe de mettre au point des technologies grâce auxquelles les organismes de renseignement pourront protéger les droits et la vie privée des Canadiens. Autrement dit, la technologie créée dans le but de tirer des renseignements de l'infrastructure mondiale d'information *doit* être complétée par une technologie pouvant être utilisée pour protéger la vie privée. C'est dans ce contexte que le besoin d'examen des activités du CST reste important.

<sup>1</sup> La Loi sur la défense nationale définit les renseignements étrangers comme suit : renseignements sur les moyens, les intentions ou les activités d'un étranger, d'un État étranger, d'une organisation étrangère ou d'un groupe terroriste étranger et qui portent sur les affaires internationales, la défense ou la sécurité (partie V.1, article 273.61).

## RÉTROSPECTIVE DE L'ANNÉE

Au cours des premiers mois qui ont suivi ma nomination, j'ai reçu plusieurs séances d'information de mon propre personnel et des fonctionnaires du CST, y compris des réunions avec le chef et son équipe exécutive, en vue de me préparer au travail que j'allais devoir faire. J'ai rencontré le ministre de la Défense nationale actuel, ainsi que son prédécesseur. J'ai également rencontré le Comité de surveillance des activités de renseignement de sécurité et le coordonnateur de la sécurité et du renseignement, qui fait en outre fonction de conseiller en matière de sécurité nationale auprès du Premier ministre et de qui relève le chef du CST pour les questions d'opérations et de politique.

Cette approche s'est révélée fructueuse par le passé et elle a souvent suscité des mesures administratives rapides. En conséquence, il a été possible d'améliorer la façon de faire les choses promptement et sans conflit. De cette manière, le processus d'examen et de rapport devient un moyen non seulement de déceler les activités illégales, mais de les prévenir. Lorsque les critiques constructives sont acceptées dans l'esprit où elles sont faites, cette approche avantage toutes les parties intéressées.

Selon cette approche, si j'avais des inquiétudes par suite d'un examen effectué par mon bureau, ma première démarche consisterait à en faire part aux personnes compétentes, soit le chef du CST et ses subordonnés. Cela leur fournirait l'occasion de prendre des mesures correctives ou de m'expliquer pourquoi mes inquiétudes sont injustifiées. J'espère que, en procédant de cette manière, la plupart des problèmes que j'aurai détectés auront déjà été résolus au moment où je présenterai des rapports classifiés au ministre de la Défense nationale, de sorte que ceux-ci auront alors perdu leur intérêt pratique.



Ce rapport est le premier que je présente à titre de commissaire du Centre de la sécurité des télécommunications (CST) depuis ma nomination, le 19 juin 2003.

Au cours des vingt années pendant lesquelles j'ai siégé à la Cour suprême du Canada, dont dix à titre de juge en chef, j'ai participé à l'évolution des droits et libertés de la personne dans notre pays, à la fois comme témoin et comme acteur, dans le cadre de nos débats touchant l'application et l'incidence de la *Charte canadienne des droits et libertés*. Cette expérience cadre très bien avec mes fonctions de commissaire du CST, car la sauvegarde des droits des Canadiens, notamment le droit à la vie privée, constitue un élément important, quoique non exhaustif, de mon mandat. Lorsque j'ai accepté cette nomination par décret, en juin dernier, j'ai donc été honoré et heureux d'avoir l'occasion de continuer à servir utilement mon pays.

Depuis ma retraite de la Cour, j'ai participé à des enquêtes et à des examens indépendants. L'un des enseignements que j'ai tirés de ces expériences a été la valeur du travail en collaboration lorsque l'on cherche à effectuer des changements et des réformes. Ces antécédents font que mon approche de l'examen des activités du Centre de la sécurité des télécommunications est essentiellement prévisionnelle et préventive. Ainsi, lorsque j'examine les opérations du CST pour m'assurer qu'on ne s'y est livré à aucune activité illégale, je cherche en outre s'il existe des contre-mesures préventives permettant d'éviter les situations où des activités illégales *pourraient* se produire. J'estime que, dans des domaines aussi fondamentaux que la sécurité et le renseignement, où la vie privée des Canadiens est en jeu, cette approche est non seulement justifiée mais essentielle pour établir l'équilibre approprié entre les exigences de la sécurité et du renseignement et les droits à la vie privée des Canadiens.



# TABLE DES MATIÈRES

1	Introduction .....
2	Rétrospective de l'année .....
4	• Autorisations régissant la collecte de renseignements étrangers .....
5	• Autorisations ministérielles .....
8	• Rapport de la vérificatrice générale du Canada .....
9	Activités de l'année 2003-2004 .....
9	• Examens relevant du mandat général du commissaire .....
9	• Examens d'activités entreprises en vertu d'autorisations ministérielles .....
10	• Examen des recommandations antérieures .....
11	• Constatations faites en 2003-2004 .....
11	• Plaintes et préoccupations au sujet des activités du CST .....
12	Le bureau du commissaire .....
12	• Dépenses du bureau et personnel .....
15	Coup d'œil sur l'avenir .....
15	• La nouvelle politique de sécurité nationale .....
16	• Mesures législatives proposées .....
18	• Conférence des organismes d'examen .....
18	Conclusion .....
19	Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications .....
21	Annexe B : État des dépenses, 2003-2004 .....
23	Annexe C : Rapports classifiés de 1996 à 2004 .....





Commissaire du Centre de la  
sécurité des télécommunications

Le très honorable Antonio Lamer,  
c.p., c.c., c.d., L.L.D., d.u.



CANADA

Communications Security  
Establishment Commissioner

The Right Honourable Antonio Lamer,  
P.C., C.C., C.D., L.L.D., D.U.

juin 2004

Ministre de la Défense nationale  
Édifice Mgén G.R. Pearkes, 13<sup>e</sup> étage  
101, promenade Colonel By, tour nord  
Ottawa (Ontario)  
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63 (3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous soumettre mon rapport annuel pour l'année 2003-2004, qui fait état de mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Antonio Lamer

P.O. Box/C.P. 1984, Station "B"/Succursale « B »  
Ottawa, Canada  
K1P 5R5  
(613) 992-3044 Fax: (613) 992-4096

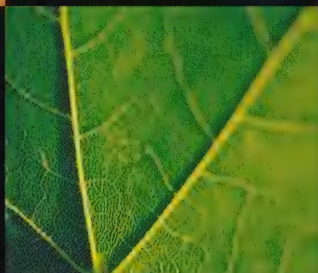
Bureau du Commissaire du Centre de la sécurité des télécommunications  
C.P. 1984, Succursale « B »  
Ottawa (Ontario)  
K1P 5R5

Tél. : (613) 992-3044

Télec. : (613) 992-4096

© Ministère des Travaux publics et des Services gouvernementaux Canada 2004  
ISBN 0-662-68250-5  
N° de cat. D95-2004

2003-2004



# Rapport annuel

COMMISSAIRE  
DU CENTRE  
DE LA SÉCURITÉ  
DES TÉLÉCOMMUNICATIONS



CA1  
ND800  
-S16



Government  
Publications

COMMUNICATIONS  
SECURITY  
ESTABLISHMENT  
COMMISSIONER

# Annual Report



2004-2005

Canada



Office of the Communications Security Establishment Commissioner  
P.O. Box 1984  
Station "B"  
Ottawa, Ontario  
K1P 5R5

Tel.: (613) 992-3044  
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2005  
ISBN 0-662-68995-X  
Cat. No. D95-2205

Communications Security  
Establishment Commissioner



The Right Honourable Antonio Lamer,  
P.C., C.C., C.D., L.L.D., D.U.

Commissaire du Centre de la  
sécurité des télécommunications

Le très honorable Antonio Lamer,  
c.p., c.c., c.d., L.L.D., d.u.

April 2005

Minister of National Defence  
1 Gen G.R. Pearkes Building, 13th Floor  
101 Colonel By Drive, North Tower  
Ottawa, Ontario  
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63 (3) of the *National Defence Act*, I am pleased  
to submit to you my 2004-2005 annual report on my activities and findings, for your submission  
to Parliament.

Yours sincerely,

Antonio Lamer

*This report is dedicated to the memory of*

Kathryn Randle

1950-2004

Our first editor



---

## TABLE OF CONTENTS

Introduction .....	1
The Year in Review .....	2
2004-2005 Activities .....	5
• The review process .....	5
• Reviews under the Commissioner's general mandate .....	6
• Reviews of activities under ministerial authorization .....	7
• Review of past recommendations .....	10
• 2004-2005 findings .....	11
• Complaints and concerns about CSE activities .....	12
The Commissioner's Office .....	12
Shaping the Review Environment .....	14
Concluding Thoughts .....	15
Annex A: Mandate of the Communications Security Establishment Commissioner .....	17
Annex B: Statement of Expenditures 2004-2005 .....	19
Annex C: Classified Reports, 1996-2005 .....	21





# INTRODUCTION

In the two years since my appointment as the Communications Security Establishment (CSE) Commissioner, an array of dramatic events has captured the world's attention, including the Cedar Revolution in Lebanon, and calls for the withdrawal of Syrian forces from that country, the Orange Revolution in the Ukraine, a renewed interest in the peace plan for Palestine, an election in Iraq, and parliamentary debates on equal rights for women in Kuwait. Meanwhile, Canada continues to deploy forces in Afghanistan so as to provide a secure environment suitable for the peaceful economic and political development of that nation. The positive scope of these political events is heartening.

Paralleling these changes in the geo-political landscape is the continued threat of terrorism globally. As evidenced by the bombings that killed or injured thousands in Madrid on March 11, 2004, international networks of terrorists continue to operate. This is the global environment in which CSE operates, one that is uncertain and volatile. At the same time, we are witnessing dramatic technological advances that, in the wrong hands, pose an ongoing threat to government information systems and assets, and ultimately, to Canada's security and economic competitiveness.

In the face of challenges such as these, CSE plays an essential role and makes a vital contribution to Canada's security and national interests. An integral part of Canada's security and intelligence community, CSE provides foreign intelligence to the Government of Canada and ensures the protection of the Government's electronic information and its information infrastructures. Today's national security realities make it imperative that CSE maintain its capacity and a high state of technological and operational readiness to meet Canada's evolving needs in these areas.

---

As the CSE Commissioner, my role is to determine if CSE's activities comply with the laws of Canada in general and, in particular, to assess whether CSE appropriately safeguards the privacy of Canadians. Over the past two years as Commissioner, I have gained an appreciation for the complex and important issues involved. Moreover, I can rely on the extensive expertise, loyalty and commitment of my staff to assist me in carrying out the Commissioner's review role effectively and efficiently.

I am pleased to submit this Annual Report for 2004-2005, summarizing the work of my office over the past year. As this report demonstrates, much has been accomplished during that time. More importantly, the report provides clear support for the essential role of the Commissioner's review function and the assurances it brings to Canadians.

## THE YEAR IN REVIEW

Largely as a result of the three-year review of Bill C-36, the omnibus *Anti-Terrorism Act*, there has been heightened attention over the past year to Canada's security and intelligence community, including CSE. When the Bill was enacted in December 2001, it resulted in key amendments to existing Acts. Of particular interest to my office were the amendments to the *Official Secrets Act* (now the *Security of Information Act*) and the *National Defence Act* (NDA). The latter provided the legislative basis for CSE and this Office. Since December 2004, this omnibus legislation has been the subject of a required three-year review by committees of the House of Commons and the Senate. I will be watching the outcome of this review with keen interest.

A number of other activities initiated during 2004-2005 have the potential to significantly affect either my office or the broader security environment in which we operate. For example, last year saw a commitment by the Prime Minister to create a National Security Committee of Parliamentarians. This commitment was made in response to a proposal set out in Canada's first-ever national security policy, which was tabled in Parliament on April 27, 2004. In this regard, an Interim Committee of Parliamentarians was struck to examine the proposal. I appeared before this committee on September 8, 2004.

Of interest to my office as well are the deliberations and outcomes of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, chaired by Mr. Justice Dennis O'Connor. In addition to investigating the role of Canadian officials in Mr. Arar's deportation from the United States to Syria, the Commission is examining options for review mechanisms for certain activities of the RCMP. I responded to the opportunity to make a submission to the Commission about some of the review options put forward. In my submission, I identified the relative strengths and weaknesses of each approach and made a recommendation on how best to proceed, given the need to safeguard the rights of persons in Canada, the realities of today's security environment and the highly sensitive nature of the RCMP's activities.

In my opinion, the most effective and logical approach is to establish one review mechanism to examine activities of the RCMP. This model would recognize the unique mandate of the RCMP, provide for a corresponding review body with the required expertise, and limit the changes required to the two organizations directly affected, the RCMP and the existing Public Complaints Commission. Furthermore, implementing this

---

structure would not affect other organizations or review groups in Canada's security and intelligence community where change in my respectful view is neither sought after nor required.

That being said, the Arar Commission's goal will be to strike an appropriate balance that is in the best interests of Canada. Again, I will be watching the deliberations with interest.

I had expressed concerns in last year's annual report about two legislative proposals: Bill C-7, the *Public Safety Act, 2002*, which introduced legislative amendments on a range of subjects, from transportation safety and immigration to biological weapons; and Bill C-14, which proposed amendments to the *Criminal Code* and the *Financial Administration Act*, among others. The concerns I had initially expressed about this legislation were later addressed. I am satisfied that as passed, the legislation establishes uniform responsibility and accountability for all departments for the protection of their computer systems and networks.

Bill C-11, the so-called *whistle-blower* legislation, was first introduced as Bill C-25 on March 22, 2004, but to date has not been passed by Parliament. Although CSE is exempt from such legislation, passage of the Bill would place an onus on CSE to establish a parallel system, with a possible review role for the Commissioner. Obviously, this legislation is of interest to me and I will continue to monitor its progress in Parliament, as well as any response by CSE.



## 2004-2005 ACTIVITIES

Each year, my office undertakes extensive reviews of CSE activities in areas that were identified as priorities as part of a multi-year workplan. Most often, these are areas within the intelligence production cycle where there is the potential for privacy issues to be raised. I report to the Minister of National Defence on all my reviews, either to provide assurance of the lawfulness of CSE activities or to bring his attention to specific concerns that arise as a result of the reviews. My activity as Commissioner properly remains confined to *ex post* review, and not to oversight, which entails a role in relation to CSE's ongoing activities.

During 2004-2005, I submitted a total of five classified reports to the Minister – two under my general review mandate and the remainder in compliance with my mandate to review specific activities authorized by the Minister.

### The review process

As in all my work, I place a high priority on collaboration during the review process. In practice, this means sharing any concerns with relevant personnel in CSE at the earliest possible stage so that appropriate corrective action can be taken, if required. As part of my office's efforts to effect change in a timely way, my staff now provide a summary briefing to all concerned CSE personnel following the review process.

One of the underlying principles guiding review is the anticipation of problem areas before they arise. That means looking beyond the issue of whether an unlawful activity has occurred, to whether one might occur and what measures can be put in place to prevent it. I believe this type of proactive and preventive approach is essential in balancing the undisputable need for security and intelligence activities with the fundamental privacy rights we have come to expect in Canada.

## Reviews under the Commissioner's general mandate

In the period covered by this report, I submitted two classified reports to the Minister of National Defence on subjects related to my general mandate to review CSE's activities to ensure they conform with the law.

One of the reports involved a review of an operational program conducted by CSE under the authority of subsection 273.64(1)(a) of the *NDA*, often referred to as CSE's foreign intelligence mandate. In this instance, my findings indicated that CSE had acted lawfully in respect of this program. Moreover, employees assigned to this program demonstrated knowledge and awareness of the relevant law and policy that governed it.

The other classified report to the Minister concerned my review of a subset of activities conducted by CSE under the authority of subsection 273.64(1)(c) of the *NDA*, in response to requests for assistance received from federal law enforcement agencies.<sup>2</sup> In this regard, the RCMP is CSE's primary client. When providing assistance to the RCMP, the scope of which is limited and defined in policy, CSE does so as an agent. Before agreeing to act in that capacity, however, CSE must first satisfy itself that the RCMP is authorized to make the request and then be satisfied that it has the authority to provide the assistance the RCMP has requested.

My office examined CSE's assistance to the RCMP under mandate (c) for the year 2003. Based on the activities reviewed, CSE's assistance was found to be in compliance with the law.

---

<sup>1</sup> See Annex A.

<sup>2</sup> 273.64(1) The mandate of the Communications Security Establishment is:  
(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

That being said, however, both reports included recommendations, many of which concerned certain weaknesses in CSE's policies and procedures, an area that has drawn similar attention and mention in previous reviews. I have also recommended that CSE accelerate efforts to improve and update existing information and records management systems. At the time of writing, CSE had resolved some of these issues and had committed to address the remainder in the coming months.

## Reviews of activities under ministerial authorization (MA)

As stated, it is my practice to conduct *ex post* review. In the case of CSE's MA-related activities, my reviews are undertaken once the authorizations in question expire.

My focus for the year under review was on activities conducted by CSE under the authority of three MAs, all of which concerned foreign intelligence collection and were the subject of classified reports to the Minister.

In conducting review activities for MAs, my office is guided directly by the legislation, which dictates what activities CSE can and cannot undertake. Specifically, my reviews in this area focus on the interception of private communications, which is what an MA authorizes. A private communication is defined in section 183 of the *Criminal Code* as

... any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone

---

communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it...

For the purpose of foreign intelligence collection, the *NDA* authorizes CSE to intercept private communications as long as the interception was the result of its having directed activities at a foreign entity located outside Canada. Over the past two years, I have focused much of my attention on foreign intelligence MAs because of their broad scope and potential degree of intrusiveness on the privacy of Canadians. While information technology security (ITS) MAs also authorize the interception of private communications, CSE seeks such authority in every instance at the request of the client agency whose systems and networks are being verified.

In my last annual report, I observed that a number of my concerns had been resolved, while some others remained. During this past year, I have been able to bring clarity to points of law and interpretation with respect to CSE's activities conducted under the authority of these provisions. My office engaged in discussions with staff and officials at CSE throughout this process.

For jurists who are accustomed to dealing with warrants issued by judges, a foreign intelligence MA is a strange sort of creature. However, one must take into account that, when collecting foreign intelligence, CSE is directing its interception efforts at foreign communications, or at least at the foreign end of communications, and a warrant issued by a Canadian court has no jurisdiction outside Canada in this instance.



Foreign intelligence MAs are a unique solution to an equally unique set of circumstances that can arise when CSE recognizes that an intercepted communication either leads into or flows out of Canada. While the interception has not been directed at a communication in Canada, one end of the communication is in Canada and is therefore, by law, a *private communication*. If this communication contains information essential to international affairs, defence or security, as specified in CSE's legislation, it is reasonable that the Government of Canada would want CSE to retain and report on it.

The foreign intelligence MA provisions in Part V.1 of the *NDA* include four conditions that must be met before the Minister of National Defence will authorize the interception of a private communication. I am of the opinion that their inclusion is both reasonable and consistent with other legislation that establishes an authority to engage in activities that would, in the absence of adequate justification, be judged an infringement on the rights of individuals as protected by the *Charter of Rights and Freedoms*.

In my view, these MA provisions are an exception to Part VI of the *Criminal Code* that protects against the invasion of privacy. I have no doubt as to their purpose because the *NDA* explicitly authorizes the interception of private communications subject to the threshold established by the four conditions, and to ministerial review. From my examination of private communications intercepted by CSE, I am able to determine if CSE has met the conditions imposed in the MA – for example, I know if the interception was a result of activities directed at a foreign entity outside of Canada. I can also determine if the communication was lawfully used, retained or destroyed – that is to say, whether or not it was



essential to the international affairs, defence or security of Canada.

In light of the above, I believe my review of activities that CSE has conducted under a foreign intelligence MA must focus on the intercepted private communications that CSE identifies to me as having been recognized and retained during the term of the authorization.

The Minister of National Defence is aware of how I have interpreted and will continue to discharge my mandate in respect of foreign intelligence MAs. I have also provided the Minister with my interpretation of the MA provisions, as currently written, and what they allow for in law. Further, I have made specific suggestions as to what could be done to remove ambiguities and to ensure a common understanding of the operational application of these provisions.

## Review of past recommendations

There is substantial evidence that I believe supports my office's review function and the impact it has had on CSE's internal processes over the years. When warranted by the review findings, I may include recommendations for action on the part of CSE. My recommendations are, appropriately, non-binding. Binding recommendations would usurp the prerogative of both the Minister, who has overall responsibility for CSE, and of the Chief of CSE, who is responsible under Part V.1 of the *NDA* for the management and control of the organization. However, one of the concerns with a review body whose recommendations are non-binding is whether that review is effective or not. I can say with confidence that review works, based on my experience with CSE's response to the recommendations made by my office.

As I outlined in my previous annual report, last year we began a process to track CSE's response to the recommendations my predecessor and I made in

classified reports submitted to the Minister of National Defence since 1996. I am pleased to provide an update. A process has also been put in place to ensure a timely response to recommendations made in upcoming reports from my office.

Over the past year, my staff worked closely with CSE to monitor their response and subsequent actions with respect to the recommendations – including establishing timetables and target dates for completion. Of the 77 recommendations made from 1996 to the end of the current fiscal year, the majority have been accepted and implemented, and I am awaiting what I believe will be a positive response from CSE on a number of others. Many of the recommendations address broad policy issues such as formalizing relations, while others focus on technical and operational practices, including ensuring consistent definitions and appropriate accountability structures. That being said, the ultimate goal of all recommendations I make is to prevent conditions or practices that have the potential to lead to unlawfulness or that could affect the privacy of Canadians. I believe that this tracking process for recommendations is fundamental to achieving this goal.

I commend the Chief of CSE on the extent to which he has accepted review as an integral part of the vision for his organization. As well, I would like to express my appreciation to CSE for their co-operation and willingness to monitor the recommendations.

## 2004-2005 findings

Each year, I state my findings about the lawfulness of CSE's activities based on the reviews my office has conducted over the past year. I am able to report that I am satisfied that the CSE activities examined during the period under review complied with the law. Moreover, I am satisfied that the intercepted private communications I examined were lawfully acquired, used and retained.

## Complaints and concerns about CSE Activities

Under Paragraph 273.63 (2)(b) of the *National Defence Act*, I am required to respond to a complaint by undertaking any investigation I consider necessary to determine whether CSE is engaging in unlawful activity. At various fora, people have expressed their surprise at the limited number of complaints directed toward my office over the years.

To my mind, the likelihood of a public complaint is diminished by the nature and focus of CSE's activities, which are technology-based and directed at foreign entities outside Canada. Unlike other federal intelligence or law enforcement agencies, CSE neither has a public profile nor engages in activities that place it in the public domain. During 2004-2005, I received no complaints about CSE activities from any source.

## THE COMMISSIONER'S OFFICE

The reviews that my office conducts are in-depth and multi-faceted, taking months to complete. I place great importance on ensuring that they are carried out with methodological rigour and consistency. Last year, I requested an internal study of my office's own review processes and I am satisfied that it employs the full range of appropriate analytical and investigative review methodologies that are best practices in the public and private sectors. Briefings, multi-level interviews, the examination of a broad range of hard and soft copy records holdings, (including authorities, policies, legal opinions and operational files), legal research, inter-agency consultation and debriefing sessions are just some of the elements that constitute this process.

During the past year, my staff also upgraded its electronic record-keeping system, known as RDIMS (records/document information management system). It is designed to improve the security, retention and access to both

non-electronic and electronic documents. This has enhanced my office's ability to track and manage its internal records.

In support of the review function, my office maintains a full-time working staff of eight, as well as a complement of contract professionals who bring a range of expertise and experience in a variety of related fields. For example, some of my staff have had considerable exposure to Canada's security and intelligence community; others have special expertise in information technology, research, policy development and communications. As a result of a multi-phase staffing initiative that was completed in June 2004, my office has been operating at full strength for almost a year. I do not anticipate further staffing requirements in the near future, provided the tempo of activity remains unchanged.

To ensure that my staff stays connected to and engaged in the broader issues facing the security and intelligence community, we host informal presentations by representatives of government and academia working in the security field. Last year, on five occasions, we invited presenters to speak about, and share in discussions on, Canadian intelligence priorities in such subject areas as terrorism, information technology and the law, and privacy.

As part of my efforts to ensure awareness of the role of the Commissioner, last year my staff – at CSE's invitation – began to give presentations to new CSE employees as part of their orientation course. This contributes directly to CSE's fulfillment of the Ministerial Directive on Accountability Framework, which is designed to ensure that CSE personnel are aware of the Commissioner's mandates of *determining whether those activities (of CSE) are in compliance with the law and of investigating complaints by citizens*,



*including CSE employees, or permanent residents of Canada concerning the lawfulness of such activities.* The Chief of CSE is also directed to ensure CSE employees extend *full support and cooperation* to the Commissioner in carrying out his mandate.

In the interests of sharing expertise and learning about timely issues, my staff attended two conferences in October 2004: the International Intelligence Review Agencies Conference (IIRAC) in Washington D.C., and the annual Canadian Association for Security Intelligence Studies (CASIS) in Ottawa. In March 2005, I was invited to participate in a symposium on Counter-terrorism and the Law held at the University of Ottawa. While I declined to be a member of the panel, I took the opportunity offered me to address the participants, and I offered a few thoughts for their consideration. In addition, and for the second year, one of my staff will participate in the National Security Studies Seminar organized by the Canadian Forces College and planned for April. These events allow for the exchange of ideas and information on issues of mutual interest and concern, and help to keep us abreast of developments in the world that affect intelligence and review.

During the past year, my office's annual expenditures were \$966,781. I am able to report that, once again, I discharged my mandated activities within budget. Annex B to this report provides a statement of my office's expenditures.

## SHAPING THE REVIEW ENVIRONMENT

It goes without saying that Canada's security and intelligence sector – as well as its various review mechanisms – will be shaped by the important parliamentary and government initiatives currently underway. As discussed earlier in this report, the ongoing three-year review of the omnibus



*Anti-Terrorism Act*, the recommendations on review mechanisms for the RCMP that are anticipated from the Arar Commission and the proposed National Security Committee of Parliamentarians, all have the potential to make a substantial impact on the security and intelligence sector over the coming months and years.

As CSE Commissioner, I will continue to monitor these initiatives carefully and, wherever possible, make a positive contribution to the outcomes. I believe that the review community has much to offer and I welcome the opportunity to be part of the process. One of the principles guiding my input will be the need for a thoughtful approach to these issues, one that does not attempt to change what works, merely for the sake of change itself. While changes may certainly be called for, we must take care not to dilute what Parliament has put in place without due consideration and reflection.

## CONCLUDING THOUGHTS

Despite the fact that the past year has posed many challenges, I look back upon it with no small degree of satisfaction. It has been a successful year. Addressing certain ambiguities in law in respect of CSE's activities under Ministerial authorizations, and establishing how my office will increase its effectiveness in reviewing them, for example, are positive steps. I am heartened by the number of recommendations made since the creation of my office that CSE has accepted and implemented, and by the ongoing dialogue between CSE and ourselves.

On a broader note, I am fully persuaded that review agencies such as my own can make an important contribution to the ongoing debate between the considerations of security and of privacy. Western democracies must make difficult choices as to where to draw the line at a time when asymmetric

---

threats are a part of our reality, and it is not an easy debate.

At a recent symposium on Counter-terrorism and the Law held at the University of Ottawa, and referred to earlier, my former colleague Supreme Court Justice Ian Binnie raised questions for discussion by the panel. He observed that the greatest threat to our rule of law is terrorism, and in matters of security it is absolutely necessary for the courts to show deference to state agencies because they have more expertise, information and resources on such matters than the courts. He questioned, however, at what point this deference should stop. While I do not have an easy answer to Mr. Justice Binnie's question, I know that it is one that merits serious contemplation given the challenges our contemporary society faces.

# Mandate of the Communications Security Establishment Commissioner

## *National Defence Act – Part V.1*

**“273.63** (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner’s activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

**“273.65 (8)** The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.”

*Security of Information Act*

**“15. (1)** No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest.

**“15. (5)** A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following:

**“15. (5) (b)** the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person’s possession to,

(ii) the Communications Security Establishment Commissioner, if the person’s concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person’s duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.”

## Statement of Expenditures 2004-2005

### Standard Object Summary

Salaries and Wages	514,130
Transportation and Telecommunications	20,688
Information	18,293
Professional and Special Services	216,889
Rentals	142,454
Purchased Repair and Maintenance	105
Materials and Supplies	8,581
Acquisition of Machinery and Equipment	45,464
Other Expenditures	177
<b>Total</b>	<b>\$966,781</b>





## **Classified Reports, 1996-2005**

Classified Report to the Minister

- March 3, 1997 (TOP SECRET)

Classified Report to the Minister

- Operational Policies with Lawfulness Implications – February 6, 1998 – (SECRET)

Classified Report to the Minister

- CSE's Activities under \*\*\* – March 5, 1998 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- Internal Investigations and Complaints – March 10, 1998 (SECRET)

Classified Report to the Minister

- CSE's activities under \*\*\* – December 10, 1998 (TOP SECRET/CEO)

Classified Report to the Minister

- On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)

Classified Report to the Minister

- How We Test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- A Study of the \*\*\* Collection Program – November 19, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- On \*\*\* – December 8, 1999 (TOP SECRET/COMINT)

Classified Report to the Minister

- A Study of the \*\*\* Reporting Process – an overview (Phase I) – December 8, 1999 (SECRET/CEO)

Classified Report to the Minister

- A Study of Selection and \*\*\* – an overview – May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's Operational Support Activities Under \*\*\* – follow-up – May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- Internal Investigations and Complaints – follow-up – May 10, 2000 (SECRET)

Classified Report to the Minister

- On findings of an external review of CSE's ITS Program – June 15, 2000 (SECRET)

Classified Report to the Minister

- CSE's Policy System Review – September 14, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- A study of the \*\*\* Reporting Process – Phase II \*\*\* – April 6, 2001 (SECRET/CEO)

Classified Report to the Minister

- A study of the \*\*\* Reporting Process – Phase III \*\*\* – April 6, 2001 (SECRET/CEO)

Classified Report to the Minister

- CSE's participation \*\*\* – August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's support to \*\*\* as authorized by \*\*\* and \*\*\* – August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister

- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – August 21, 2002 (SECRET)

Classified Report to the Minister

- CSE's support to XXX, as authorized by \*\*\* and code named \*\*\* – November 13, 2002 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's SIGINT activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)

Classified Report to the Minister

- Lexicon – 26 March 2003 (TOP SECRET/COMINT)

Classified Report to the Minister

- CSE's activities pursuant to three XXX Ministerial authorizations including \*\*\*  
\*\*\* – May 20, 2003 (SECRET)

Classified Report to the Minister

- CSE's support to XXX, as authorized by \*\*\* and code named \*\*\* – Part I –  
November 6, 2003 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister

- CSE's support to XXX, as authorized by \*\*\* and code named \*\*\* – Part II –  
March 15, 2004 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister

- A review of CSE's activities conducted under XXX Ministerial authorization –  
March 19, 2004 (SECRET/CEO)

Classified Report to the Minister

- Internal investigations and complaints – follow-up – March 25, 2004  
(TOP SECRET/CEO)

Classified Report to the Minister

- A review of CSE's activities conducted under XXX Ministerial authorization –  
April 19, 2004 (SECRET/CEO)

Classified Report to the Minister

- Review of CSE XXX Operations under Ministerial authorization –  
June 1, 2004 (TOP SECRET/COMINT)

Classified Report to the Minister

- CSE's Support to XXX – January 7, 2005 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister

- External Review of CSE's XXX Activities Conducted Under Ministerial  
authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister

- A Study of the XXX Collection Program – March 15, 2005 (TOP SECRET/  
COMINT/CEO)

Classified Report to the Minister  
– Lexicon – 26 mars 2003 (TRÈS SECRET/COMINT)

Classified Report to the Minister  
– CSE's activities pursuant to three XXX ministerial authorizations including  
\*\*\*\*\* – 20 mai 2003 (SECRET)

Classified Report to the Minister  
– CSE's support to XXX, as authorized by \*\*\* and code named \*\*\* – Part I – N  
6 novembre 2003 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

Classified Report to the Minister  
– CSE's support to XXX, as authorized by \*\*\* and code named \*\*\* – Part II –  
15 mars 2004 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

Classified Report to the Minister  
– A review of CSE's activities conducted under XXX Ministerial authorization –  
19 mars 2004 (SECRET/Réserve aux Canadiens)

Classified Report to the Minister  
– Internal investigations and complaints – Follow-up – 25 mars 2004  
(TRÈS SECRET/Réserve aux Canadiens)

Classified Report to the Minister  
– A review of CSE's activities conducted under XXX Ministerial authorization –  
19 avril 2004 (SECRET/Réserve aux Canadiens)

Classified Report to the Minister  
– Review of CSE XXX Operations under Ministerial authorization –  
1<sup>er</sup> juin 2004 (TRÈS SECRET/COMINT)

Classified Report to the Minister  
– CSE's Support to XXX – 7 janvier 2005 (TRÈS SECRET/COMINT/  
Réserve aux Canadiens)

Classified Report to the Minister  
– External Review of CSE's XXX Activities Conducted Under Ministerial  
authorization – 28 février 2005 (TRÈS SECRET/COMINT/Réserve aux  
Canadiens)

Classified Report to the Minister  
– A Study of the XXX Collection Program – 15 mars 2005 (TRÈS SECRET/  
COMINT/Réserve aux Canadiens)



- Classified Report to the Minister  
– CSE's Operational Support Activities Under \*\*\* – follow-up – 10 mai 2000 (TRÈS SECRET/Réserve aux Canadiens)
- Classified Report to the Minister  
– Internal Investigations and Complaints – follow-up – 10 mai 2000 (SECRET)
- Classified Report to the Minister  
– On findings of an external review of CSE's ITS Program – 15 juin 2000 (SECRET)
- Classified Report to the Minister  
– CSE's Policy System Review – 14 septembre 2000 (TRÈS SECRET/Réserve aux Canadiens)
- Classified Report to the Minister  
– A study of the \*\*\* Reporting Process – Phase II \*\*\* – 6 avril 2001 (SECRET/Réserve aux Canadiens)
- Classified Report to the Minister  
– A study of the \*\*\* Reporting Process – Phase III \*\*\* – 6 avril 2001 (SECRET/Réserve aux Canadiens)
- Classified Report to the Minister  
– CSE's participation \*\*\* – 20 août 2001 (TRÈS SECRET/Réserve aux Canadiens)
- Classified Report to the Minister  
– CSE's support to \*\*\*, as authorized by \*\*\* and \*\*\* – 20 août 2001 (TRÈS SECRET/Réserve aux Canadiens)
- Classified Report to the Minister  
– A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – 20 août 2002 (SECRET)
- Classified Report to the Minister  
– CSE's support to XXX as authorized by \*\*\* and code named \*\*\* – 13 novembre 2002 (TRÈS SECRET/Réserve aux Canadiens)
- Classified Report to the Minister  
– CSE's SIGINT activities carried out under the \*\*\* 2002 \*\*\* ministerial authorization – 27 novembre 2002 (TRÈS SECRET/Réserve aux Canadiens)

## Rapports classifiés de 1996 à 2005

Classified Report to the Minister  
– 3 mars 1997 (TRÈS SECRET)

Classified Report to the Minister  
– Operational Policies with Lawfulness Implications – 6 février 1998 – (SECRET)

Classified Report to the Minister  
– CSE's activities under \*\*\* – 5 mars 1998 (TRÈS SECRET Mot code/Réservé aux Canadiens)

Classified Report to the Minister  
– Internal Investigations and Complaints – 10 mars 1998 (SECRET)

Classified Report to the Minister  
– CSE's activities under \*\*\* – 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister  
– On controlling communications security (COMSEC) material – 6 mai 1999 (TRÈS SECRET)

Classified Report to the Minister  
– How We Test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) – 14 juin 1999 (TRÈS SECRET Mot code/Réservé aux Canadiens)

Classified Report to the Minister  
– A Study of the \*\*\* Collection Program – 19 novembre 1999 (TRÈS SECRET Mot code/Réservé aux Canadiens)

Classified Report to the Minister  
– On \*\*\* – 8 décembre 1999 (TRÈS SECRET/COMINT)

Classified Report to the Minister  
– A Study of the \*\*\* Reporting Process – an overview (Phase I) – 8 décembre 1999 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister  
– A Study of Selection and \*\*\* – an overview – 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)



Sommaire des articles courants	
Traitements et salaires	514 130
Transports et télécommunications	20 688
Information	18 293
Services professionnels et spéciaux	216 889
Location	142 454
Achat de services de réparation et d'entretien	105
Fournitures et approvisionnements	8 581
Acquisition de machines et de matériel	45 464
Autres charges	177
<b>Total</b>	<b>966 781 \$</b>

*Loi sur la protection de l'information*

« 273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre. »

« 15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public.

« 15. (5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes :

« 15. (5) (b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession :

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable. »



« 273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

(a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

(b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

(c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

Lors du récent symposium sur l'antiterrorisme et le droit tenu à l'Université d'Ottawa et dont je fais mention plus haut, mon ancien collègue de la Cour suprême, le juge Ian Binnie, a soumis des questions au groupe d'experts. Il a fait remarquer que la plus grande menace pour la primauté du droit dans notre société est le terrorisme et que, en matière de sécurité, les tribunaux doivent absolument s'en remettre aux organismes de l'Etat parce que ceux-ci possèdent plus de connaissances, d'information et de ressources que les tribunaux dans ce domaine. Il a cependant demandé jusqu'où cela devait aller. Je n'ai pas de réponse facile à lui donner, mais je sais que sa question mérite un examen sérieux mené en regard des défis que soulève la situation contemporaine.

## DERNIÈRES RÉFLEXIONS

À titre de commissaire du CST, je continuerai de surveiller ces initiatives de près et, dans tous les cas où ce sera possible, d'apporter une contribution positive aux résultats. Je pense que la collectivité de l'examen a beaucoup à offrir, et je me réjouis d'avoir l'occasion de participer au processus. L'un des principes qui guidera mon apport sera l'importance d'un examen sérieux de ces questions, qui ne cherche pas à changer ce qui fonctionne bien pour le simple plaisir de changer. Des changements pourront certes être justifiés, mais nous devons faire attention à ne pas diluer ce que le Parlement a mis en place, sans y avoir mûrement réfléchi.

Même si l'année écoulée a présenté de nombreux défis, je l'évoque avec beaucoup de satisfaction. Ça a été une année réussie, marquée de réalisations fructueuses. Ainsi, nous avons résolu certaines ambiguïtés de droit touchant les activités menées par le CST en vertu d'autorisations ministérielles et nous avons trouvé des moyens d'accroître l'efficacité avec laquelle mon bureau les examine. Je suis encouragé par le nombre de recommandations qui, depuis la création de mon bureau, ont été acceptées et mises en œuvre par le CST, ainsi que par le dialogue suivi entre celui-ci et notre équipe.

Dans un ordre d'idées plus général, je suis convaincu que les organismes d'examen comme le nôtre peuvent apporter une contribution importante au débat en cours sur les considérations de sécurité et de protection de la vie privée. Les démocraties occidentales doivent faire des choix difficiles et déterminer où fixer les limites à une époque où les menaces asymétriques font partie de la réalité. Ce n'est pas un débat facile.

## MODELER LE CONTEXTE D'EXAMEN

(CASIS), à Ottawa. En mars 2005, j'ai été invité à participer à un symposium sur l'antiterrorisme et le droit, tenu à l'Université d'Ottawa. J'ai refusé de faire partie du groupe d'experts, mais j'ai profité de l'occasion qui m'était offerte d'adresser la parole aux participants et j'ai soumis quelques réflexions à leur examen. De plus, pour la deuxième année, un de mes collaborateurs participera au Séminaire des études de sécurité nationale organisé par le Collège des Forces canadiennes, qui doit se tenir en avril. Ces activités favorisent l'échange d'idées et d'information sur des questions d'intérêt mutuel et contribuent à nous tenir au courant des faits nouveaux dans le monde, qui ont des incidences dans le domaine du renseignement et de l'examen. Au cours de la dernière année, les dépenses de mon bureau ont été de 966 781 \$. Je suis à même de signaler que je me suis de nouveau acquitté de mon mandat dans le cadre de mon budget. On trouvera à l'annexe B un état des dépenses de mon bureau.

Il va sans dire que le secteur canadien de la sécurité et du renseignement – de même que ses divers mécanismes d'examen – sera modelé par les importantes initiatives parlementaires et gouvernementales actuellement en cours. Comme je le mentionne plus haut, l'examen triennal en cours de la *Loi antiterroriste*, les recommandations relatives aux mécanismes d'examen de la GRC qui, prévoit-on, seront formulées par la Commission Arar, et la proposition de création d'un comité de parlementaires sur la sécurité nationale pourraient tous avoir une incidence importante sur le secteur de la sécurité et du renseignement au cours des prochains mois et des prochaines années.

Pour que les membres de mon personnel demeurent au courant des grandes questions auxquelles est confrontée la collectivité de la sécurité et du renseignement et continuent de se sentir concernés, nous invitons des représentants des services gouvernementaux et des universités travaillant dans le domaine de la sécurité à leur donner des présentations informelles. L'année dernière, nous avons accueilli à cinq reprises des conférenciers qui sont venus traiter et discuter des priorités canadiennes en matière de renseignement dans des domaines comme le terrorisme, la technologie de l'information et le droit, et la protection de la vie privée.

Dans le cadre de mes efforts pour faire connaître le rôle du commissaire, mon personnel a commencé l'année dernière – à l'invitation du CST – à donner des exposés aux nouveaux employés du CST dans le cadre de leur cours d'orientation. Cette initiative contribue directement à l'exécution de la directive ministérielle sur le cadre de responsabilité, qui vise à assurer que le personnel du CST est au courant des mandats du commissaire de déterminer si ces activités (du CST) sont conformes à la loi et d'enquêter sur les plaintes de citoyens, dont des employés du CST, ou de résidents permanents du Canada concernant la légalité de ces activités. Le chef du CST a en outre pour instruction de veiller à ce que les employés du Centre apportent un appui et une coopération complets au commissaire dans l'exécution de son mandat.

Dans le but de communiquer leur expertise et leur savoir sur des questions d'actualité, des membres de mon personnel ont participé à deux conférences tenues en octobre 2004, soit la conférence internationale des organismes d'examen des activités de renseignement, à Washington (D.C.), et la conférence annuelle de l'Association canadienne pour l'étude du renseignement et de la sécurité



méthodes d'examen analytiques et d'investigation appropriées qui constituent des pratiques exemplaires dans le secteur public comme dans le secteur privé. Les séances d'information, les entrevues à plusieurs niveaux, l'examen d'un grand nombre de fonds de dossiers imprimés et électroniques (dont les autorisations, les politiques, les avis juridiques et les dossiers opérationnels), la recherche juridique, la consultation entre organismes et les séances de comptes rendus ne sont que quelques-uns des éléments constitutifs de ce processus.

Au cours de l'année dernière, mon personnel a par ailleurs amélioré son système électronique de tenue de dossiers, ou SGDDI (système de gestion des dossiers, des documents et de l'information). Ce système est conçu pour améliorer la sécurité et la conservation des documents non électroniques et électroniques ainsi que l'accès à ceux-ci. Mon bureau a ainsi amélioré sa capacité de suivre et de gérer ses dossiers internes.

À l'appui de la fonction d'examen, mon bureau continue d'avoir à son service huit employés à plein temps ainsi qu'un effectif de professionnels engagés par contrat qui possèdent un bagage d'expertise et d'expérience dans divers domaines connexes. Par exemple, certains de mes collaborateurs ont eu de nombreux contacts avec la collectivité canadienne de la sécurité et du renseignement; d'autres possèdent des connaissances spécialisées en technologies de l'information, en recherche, en élaboration des politiques et en communications. Par suite d'une initiative de dotation en plusieurs étapes qui a été achevée en juin 2004, mon bureau fonctionne avec un plein effectif depuis près d'une année. Je ne prévois pas de nouveaux besoins en personnel dans un avenir rapproché, pourvu que le rythme d'activité reste inchangé.

Chaque année, je présente mes constatations au sujet de la légalité des activités du CST en me fondant sur les examens effectués par mon bureau au cours des 12 mois précédents. Je suis en mesure de rapporter que je suis persuadé que les activités du CST examinées au cours de la période visée ont été conformes à la loi. De plus, je suis convaincu que les communications privées interceptées que j'ai examinées avaient été acquises, utilisées et conservées légalement.

Conformément à l'alinéa 273.63(2)b) de la *Loi sur la défense nationale*, je dois répondre à une plainte en effectuant toute enquête que je juge nécessaire pour déterminer si le CST se livre à une activité illégale. Sur des tribunes diverses, des gens ont exprimé leur surprise au sujet du nombre limité de plaintes adressées à mon bureau au fil des ans.

À mon sens, la probabilité d'une plainte du public est réduite du fait de la nature et de l'objet des activités du CST, qui se fondent sur la technologie et visent des entités étrangères situées à l'extérieur du Canada. Contrairement aux autres organismes fédéraux de renseignement ou d'application de la loi, le CST n'a aucune visibilité publique et il ne se livre pas non plus à des activités qui le placent dans le domaine public. Au cours de l'année 2004-2005, je n'ai reçu de plainte d'aucune source au sujet des activités du CST.

Les examens qu'effectue mon bureau sont approfondis et multidimensionnels, et ils exigent des mois de travail. Il est, à mon sens, très important de m'assurer qu'ils sont exécutés de manière rigoureuse et uniforme. L'année dernière, j'ai demandé une étude interne des propres processus d'examen de mon bureau, et je suis convaincu qu'il emploie toute la gamme des

Comme je le mentionnais dans mon rapport annuel précédent, nous avons entrepris l'année dernière un travail de suivi de la réaction du CST aux recommandations que mon prédécesseur et moi-même avions faites dans des rapports classifiés présentés au ministre de la Défense nationale depuis 1996. Je suis heureux de rendre compte de ce travail. Un processus a aussi été mis en place pour faire en sorte que le Centre donne rapidement suite aux recommandations que formulera mon bureau dans les rapports à venir.

Au cours de l'année dernière, mon personnel a travaillé étroitement avec les gens du CST pour surveiller leur réaction et les mesures prises à la suite des recommandations, notamment l'établissement de calendriers et de dates cibles d'achèvement. Sur les 77 recommandations faites entre 1996 et la fin de la présente année financière, la majorité ont été acceptées et mises en œuvre, et j'attends ce qui, je pense, sera une réponse positive du CST sur un certain nombre d'autres. Nombre de recommandations portent sur des grandes questions de principe comme l'officialisation des relations, tandis que d'autres touchent les pratiques techniques et opérationnelles, dont l'établissement de définitions uniformes et de structures de responsabilité appropriées. Cela dit, le but final de toutes mes recommandations est de prévenir les situations ou les pratiques qui pourraient mener à l'illégalité ou avoir une incidence sur la vie privée des Canadiens. Je pense que ce processus de suivi des recommandations est fondamental pour atteindre ce but.

Je salue la mesure dans laquelle le chef du CST a accepté l'examen en tant que partie intégrante de la vision de son organisation. Je tiens en outre à exprimer ma reconnaissance aux gens du CST pour leur coopération et leur volonté de donner suite aux recommandations.

À la lumière de ce qui précède, je pense que mon examen des activités menées par le CST en vertu d'une AM visant l'obtention de renseignements étrangers doit porter sur les communications privées interceptées dont le CST m'indique qu'elles ont été reconnues et conservées pendant la durée de l'autorisation.

Le ministre de la Défense nationale sait comment j'ai interprété et je continuerai de remplir mon mandat à l'égard des AM visant l'obtention de renseignements étrangers. J'ai par ailleurs fourni au ministre mon interprétation des dispositions relatives aux AM, telles qu'elles sont actuellement libellées, et de ce qu'elles permettent en droit. J'ai en outre présenté des suggestions particulières sur ce que l'on pourrait faire pour supprimer les ambiguïtés et assurer une compréhension commune de l'application de ces dispositions en pratique.

## Examen de recommandations passées

Je pense qu'il existe des preuves concluantes à l'appui de la fonction d'examen de mon bureau et de l'incidence qu'elle a eue sur les processus internes du CST au fil des ans. Lorsque les constatations de l'examen le justifient, j'inclus parfois des recommandations de mesures à prendre par le CST. Ces recommandations sont, comme il se doit, non obligatoires. Des recommandations obligatoires usurperaient à la fois la prérogative du ministre, qui a la responsabilité d'ensemble du CST, et celle du chef du CST, qui est responsable de la gestion du Centre en vertu de la partie V.1 de la LDN. L'efficacité de l'examen effectué par un organisme dont les recommandations ne sont pas obligatoires pourrait être mise en doute. Toutefois, en me fondant sur mon expérience de la réaction du CST aux recommandations faites par mon bureau, je peux affirmer avec assurance que l'examen est efficace.



Canada et est par conséquent, selon la loi, une *communication privée*. Si cette communication contient de l'information essentielle aux affaires internationales, à la défense ou à la sécurité, comme le précise la loi intéressant le CST, il est raisonnable que le gouvernement du Canada veuille que le CST la conserve et en fasse rapport.

Les dispositions relatives aux AM visant l'obtention de renseignements étrangers, qui figurent à la partie V.1 de la LDN, comprennent quatre conditions qui doivent être remplies avant que le ministre de la Défense nationale autorise l'interception d'une communication privée. Je suis d'avis que l'inclusion de ces conditions est à la fois raisonnable et compatible avec les autres lois qui établissent un pouvoir d'exercer des activités en l'absence de justification suffisante, seraient considérées comme un empiètement sur les droits de la personne garantis par la *Charte canadienne des droits et libertés*.

À mon avis, ces dispositions sur les AM constituent une exception à la partie VI du *Code criminel*, qui protège contre l'intrusion dans la vie privée. Je n'ai aucun doute quant à leur but, car la LDN autorise explicitement l'interception de communications privées sous réserve des quatre conditions et de l'examen ministériel. Mon examen des communications privées interceptées par le CST me permet de déterminer s'il a satisfait aux conditions imposées dans l'AM; par exemple, je sais si l'interception a été le résultat d'activités visant une entité étrangère située à l'extérieur du Canada. Je peux également déterminer si la communication a été utilisée, conservée ou détruite conformément à la loi, c'est-à-dire si oui ou non elle était essentielle aux affaires internationales, à la défense ou à la sécurité du Canada.



Canada. Au cours des deux dernières années, j'ai accordé beaucoup d'attention aux AM sur les renseignements étrangers en raison de leur vaste portée et du degré possible d'immixtion dans la vie privée de Canadiens. Les AM relatives à la sécurité des technologies de l'information (STI) autorisent également l'interception de communications privées, mais le CST sollicite cette autorisation dans tous les cas à la demande de l'organisme client dont les systèmes et les réseaux font l'objet d'une vérification.

Dans mon dernier rapport annuel, je signalais qu'un certain nombre de mes préoccupations avaient été résolues, tandis que d'autres subsistaient. Au cours de la dernière année, j'ai pu faire clarifier des points de droit et d'interprétation relatifs aux activités que mène le CST en vertu de ces dispositions. Mon bureau a eu des entretiens avec des membres du personnel et des cadres du CST tout au long de ce processus.

Pour les juristes qui sont habitués aux mandats émis par des juges, une AM relative à des renseignements étrangers peut surprendre. Toutefois, il faut tenir compte du fait que, lorsqu'il recueille des renseignements étrangers, le CST cherche à intercepter des communications étrangères, ou au moins la portion étrangère de ces communications, et qu'un mandat délivré par un tribunal canadien n'a pas compétence en dehors du Canada dans ce cas.

Les AM relatives à des renseignements étrangers sont une solution unique que l'on applique à un ensemble également unique de circonstances qui peuvent survenir lorsque le CST reconnaît que l'origine ou la destination d'une communication interceptée se trouve au Canada. L'interception ne visait pas une communication au Canada, mais l'un des pôles de la communication se trouve au

## Examens d'activités découlant d'une autorisation ministérielle (AM)

Comme je l'ai dit, j'effectue des examens *a posteriori*. Dans le cas des activités du CST autorisées par le ministre, j'entreprends mes examens une fois que les autorisations en question arrivent à terme.

Au cours de l'année à l'étude, je me suis concentré sur les activités menées par le CST en vertu de trois AM; ces activités avaient toutes trait à la collecte de renseignements étrangers et ont fait l'objet de rapports classifiés au ministre.

Lorsqu'il examine des activités menées en vertu d'AM, mon bureau est guidé directement par la législation, qui prescrit les activités permises et interdites au CST. Plus précisément, mes examens dans ce domaine portent sur l'interception de communications privées, qui sont ce qu'une AM autorise. L'article 183 du *Code criminel* définit une communication privée comme suit :

Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.

Aux fins de la collecte de renseignements étrangers, la LDN autorise le CST à intercepter des communications privées à condition que l'interception résulte d'activités par lesquelles il vise une entité étrangère située à l'extérieur du

constatations ont révélé que le CST avait agi légalement dans le cadre de ce programme. De plus, les employés affectés avaient montré qu'ils connaissaient bien la loi et la politique qui le régissent.

L'autre rapport classifié au ministre avait trait à mon examen d'un sous-ensemble d'activités menées par le CST en vertu de l'alinéa 273.64(1)c) de la LDN, pour répondre aux demandes d'aide reçues d'organismes fédéraux d'application de la loi<sup>2</sup>. À cet égard, la GRC est le principal client du CST. Lorsqu'il fournit à la GRC une aide dont la portée est limitée et définie dans une politique, le CST le fait à titre d'agent. Avant d'accepter d'agir à ce titre, il doit cependant s'assurer, d'une part, que la GRC est autorisée à faire la demande et, d'autre part, qu'il a le pouvoir de fournir l'aide en question.

Mon bureau a examiné l'aide fournie par le CST à la GRC en vertu du mandat c) pour l'année 2003. En se fondant sur les activités examinées, il a conclu que cette aide avait été conforme à la loi.

Cela dit, toutefois, les deux rapports contenaient des recommandations dont beaucoup avaient trait à certaines faiblesses des politiques et procédures du CST, domaine qui a fait l'objet d'une attention et de mentions semblables lors d'examens précédents. J'ai en outre recommandé que le CST accélère ses efforts pour améliorer et actualiser les systèmes actuels de gestion de l'information et des dossiers. Au moment de la rédaction du présent rapport, le CST avait résolu certaines de ces questions et s'était engagé à s'occuper des autres au cours des mois à venir.

<sup>2</sup> 273.64(1) Le mandat du Centre de la sécurité des télécommunications est

le suivant :

(c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère.

## Le processus d'examen

## Examens effectués dans le cadre du mandat général du commissaire

Comme dans tout mon travail, j'accorde une haute priorité à la collaboration au cours du processus d'examen. En pratique, cela veut dire faire part de mes préoccupations au personnel concerné du CST le plus tôt possible, afin que des mesures correctrices appropriées puissent être prises s'il y a lieu. Dans le cadre des efforts déployés par mon bureau pour effectuer des changements de manière opportune, mes collaborateurs donnent maintenant, à la suite du processus d'examen, une séance d'information sommaire à tout le personnel concerné du CST.

L'un des principes fondamentaux qui guident l'examen consiste à repérer les secteurs

problématiques avant qu'un problème ne se manifeste. Ainsi il s'agit de chercher à savoir non seulement s'il y a eu activité illégale, mais encore si une telle activité serait possible et si des mesures préventives peuvent être mises en place pour la prévenir. Je pense que cette approche proactive et préventive est essentielle pour établir un équilibre entre le besoin indiscutable d'activités de sécurité et de renseignement et les droits fondamentaux à la vie privée que nous nous attendons à voir garantis au Canada.

Au cours de la période couverte par le présent rapport, j'ai présenté deux rapports classifiés au

ministre de la Défense nationale sur des sujets liés à mon mandat général<sup>1</sup> d'examiner les activités du CST pour en vérifier la légalité.

L'un des rapports portait sur l'examen d'un

programme opérationnel mis en œuvre par le CST en vertu de l'alinéa 273.64(1)a) de la LDN, souvent désigné comme le mandat du CST en matière de renseignement étranger. Dans ce cas, mes

<sup>1</sup> Voir l'annexe A.

Le projet de loi C-11 (la loi dite de la dénonciation) a initialement été déposé sous le nom de projet de loi C-25 le 22 mars 2004, mais il n'a pas encore été adopté par le Parlement. Cette loi ne vise pas le CST, mais, si elle était adoptée, le Centre serait obligé d'établir un système parallèle qui devrait peut-être être soumis à l'examen du commissaire. Manifestement, ce projet de loi m'intéresse, et je continuerai de surveiller son cheminement au Parlement, ainsi que toute réaction du CST.

Chaque année, mon bureau procède à des examens approfondis des activités du CST dans des domaines désignés prioritaires dans un plan de travail pluriannuel. Le plus souvent, il s'agit de domaines touchant le cycle de production du renseignement où des questions de protection de la vie privée risquent d'être soulevées. Je rends compte de tous mes examens au ministre de la Défense nationale, soit pour l'assurer de la légalité des activités du CST, soit pour lui signaler des préoccupations particulières découlant des examens. Mon travail de commissaire se limite à juste titre à un examen *a posteriori*; je n'exerce pas de surveillance, ce qui supposerait un rôle relativement aux activités courantes du CST.

Au cours de l'année 2004-2005, j'ai présenté en tout cinq rapports classifiés au ministre, soit deux dans le cadre de mon mandat général et les trois autres conformément à mon mandat d'examiner des activités particulières autorisées par le ministre.



sécurité et de la nature très délicate des activités de la GRC.

À mon avis, l'approche la plus efficace et la plus logique consiste à établir un mécanisme de contrôle unique des activités de la GRC. Ce modèle reconnaîtrait le mandat singulier de celle-ci, prévoirait un organe d'examen correspondant possédant l'expertise nécessaire et limiterait les modifications à apporter aux deux organisations directement concernées, soit la GRC et l'actuelle Commission des plaintes du public. De plus, l'instauration de cette structure ne toucherait pas d'autres organisations ni groupes d'examen de la collectivité canadienne du renseignement et de la sécurité où des changements ne sont ni recherchés ni nécessaires.

Cela dit, la Commission Arar s'efforcera de trouver un équilibre adéquat, qui servira au mieux les intérêts du Canada. Ici encore, je suivrai les délibérations avec intérêt.

Dans mon rapport de l'année dernière, j'avais exprimé des préoccupations au sujet de deux mesures législatives proposées, soit le projet de loi C-7, *Loi de 2002 sur la sécurité publique*, qui prévoyait des modifications législatives sur plusieurs sujets, de la sécurité des transports à l'immigration en passant par les armes biologiques, et le projet de loi C-14, qui prévoyait entre autres des modifications du *Code criminel* et de la *Loi sur la gestion des finances publiques*. Ces préoccupations initiales ont été prises en compte par la suite, et je suis persuadé que les lois adoptées prévoient une responsabilité et une responsabilisation uniformes pour tous les ministères en ce qui concerne la protection de leurs systèmes et de leurs réseaux informatiques.

et de la *Loi sur la défense nationale* (LDN). Cette dernière a fourni le fondement législatif du CST et de mon bureau. Depuis décembre 2004, la loi omnibus fait l'objet d'un examen triennal obligatoire par des comités de la Chambre des communes et du Sénat. Je me pencherai avec un vif intérêt sur les résultats de cet examen.

Un certain nombre d'autres activités entreprises au cours de l'année 2004-2005 pourraient avoir une incidence importante sur mon bureau ou sur le contexte plus général de la sécurité dans lequel nous œuvrons. Par exemple, le Premier ministre s'est engagé, l'année dernière, à créer un comité de parlementaires sur la sécurité nationale. Il a pris cet engagement en réponse à une proposition figurant dans la toute première politique sur la sécurité nationale du Canada, qui a été déposée au Parlement le 27 avril 2004. Un comité provisoire de parlementaires avait été constitué pour examiner cette proposition. J'ai comparu devant ce comité le 8 septembre 2004.

Les délibérations et les conclusions de la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, présidée par M. le juge Dennis O'Connor, intéressent également mon bureau. En plus d'enquêter sur le rôle des fonctionnaires canadiens relativement à l'expulsion de M. Arar des États-Unis en Syrie, la Commission examine différents mécanismes qui permettraient de contrôler certaines activités de la GRC. J'ai eu l'occasion de présenter un mémoire à la Commission au sujet de certaines des options proposées. J'y ai recensé les forces et les faiblesses relatives de chaque approche et fait une recommandation sur la meilleure façon de procéder, compte tenu de la nécessité de protéger les droits des personnes se trouvant au Canada, des réalités du contexte actuel de la

## RÉTROSPECTIVE DE L'ANNÉE

d'information. Compte tenu des réalités actuelles de la sécurité nationale, il est impératif que le CST conserve sa capacité et un haut degré de préparation technologique et opérationnelle pour répondre aux besoins changeants du Canada dans ces domaines. En ma qualité de commissaire du CST, mon rôle consiste à déterminer si les activités du Centre respectent les lois du Canada en général et, en particulier, à évaluer s'il protège convenablement la vie privée des Canadiens. Dans l'exercice de mes fonctions au cours des deux dernières années, j'ai pu apprécier la complexité et l'importance des questions en cause. Je peux par ailleurs compter sur les connaissances étendues, la loyauté et le dévouement de mon personnel pour m'aider à m'acquitter de mon rôle d'examen de manière efficace et efficiente.

Je suis heureux de présenter ce rapport annuel pour 2004-2005, qui résume le travail accompli par mon bureau au cours de l'année écoulée. Comme ce document le révèle, ce travail a été considérable. Chose plus importante, il appuie clairement le caractère essentiel de la fonction d'examen du commissaire et les assurances qu'elle apporte aux Canadiens.

Au cours de l'année écoulée, on a prêté une attention accrue à la collectivité canadienne de la sécurité et du renseignement, dont le CST, en grande partie par suite de l'examen triennal du projet de loi omnibus C-36, ou *Loi antiterroriste*. L'adoption du projet de loi, en décembre 2001, a entraîné des modifications fondamentales de lois existantes qui avaient toutes pour but de renforcer la capacité du Canada de combattre le terrorisme. Mon bureau était particulièrement intéressé par les modifications de la *Loi sur les secrets officiels* (désormais *Loi sur la protection de l'information*)

Au cours des deux années qui se sont écoulées depuis ma nomination au poste de commissaire du Centre de la sécurité des télécommunications (CST), une série d'événements dramatiques ont capté l'attention du monde, entre autres la révolution des cédres au Liban et les demandes de retrait des forces syriennes de ce pays, la révolution orange en Ukraine, un intérêt renouvelé pour le plan de paix pour la Palestine, les élections en Iraq, et les débats parlementaires sur l'égalité des droits des femmes au Koweït. Entre-temps, le Canada a continué de déployer des forces en Afghanistan afin de ménager un environnement sûr, propice au développement économique et politique pacifique de ce pays. La portée positive de ces événements politiques est encourageante.

La menace continue de terrorisme à l'échelle mondiale fait pendant à cette évolution du contexte géopolitique. Comme en témoignent les attentats à la bombe qui ont tué ou blessé des milliers de personnes à Madrid, le 11 mars 2004, les réseaux internationaux de terroristes continuent d'opérer. C'est dans ce contexte mondial incertain et volatil que le CST exerce ses activités. Parallèlement, nous sommes témoins de progrès technologiques spectaculaires qui, s'ils tombaient dans de mauvaises mains, présenteraient une menace permanente pour les systèmes et les fonds d'information du gouvernement et, en fin de compte, pour la sécurité et la compétitivité économique du Canada.

Face à de tels défis, le CST joue un rôle essentiel et apporte une contribution capitale à la sécurité et aux intérêts nationaux du Canada. Le CST, qui fait partie intégrante de la collectivité canadienne de la sécurité et du renseignement, fournit des renseignements étrangers au gouvernement du Canada et assure la protection des renseignements électroniques de l'État et de son infrastructure





TABLE DES MATIÈRES

Introduction .....	1
.....	2
.....	5
.....	6
.....	6
.....	8
.....	11
.....	13
.....	13
.....	13
.....	16
.....	17
.....	19
.....	21
.....	23

*Ce rapport est dédié à la mémoire de*

Kathryn Randle

1950-2004

notre première rédactrice

Commissaire du Centre de la  
sécurité des télécommunications

Le très honorable Antonio Lamer,  
c.p., c.c., c.d., L.L.D., d.u.



Communications Security  
Establishment Commissioner

The Right Honourable Antonio Lamer,  
P.C., C.C., C.D., L.L.D., D.U.

Avril 2005

ministre de la Défense nationale  
Office Mgén G.R. Parkes, 13<sup>e</sup> étage  
1, promenade Colonel By, tour nord  
Ottawa (Ontario)  
A 0K2

onsieur le Ministre,

Conformément au paragraphe 273.63 (3) de la *Loi sur la défense nationale*, j'ai le  
suisir de vous soumettre mon rapport annuel pour l'année 2004-2005, qui fait état de mes activités et  
statations, aux fins de présentation au Parlement.  
Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Antonio Lamer

P.O. Box/C.P. 1984, Station "B"/Succursale « B »  
Ottawa, Canada  
K1P 5R5  
(613) 992-3044 Téléc. : (613) 992-4096

Bureau du Commissaire du Centre de la sécurité des télécommunications  
C.P. 1984, Succursale « B »  
Ottawa (Ontario)  
K1P 5R5

Tél. : (613) 992-3044

Télec. : (613) 992-4096

© Ministère des Travaux publics et des Services gouvernementaux Canada 2005  
ISBN 0-662-68995-X  
N° de cat. D95-2005

2004-2005



# Rapport annuel

COMMISSAIRE  
DU CENTRE  
DE LA SÉCURITÉ  
DES TÉLÉCOMMUNICATIONS





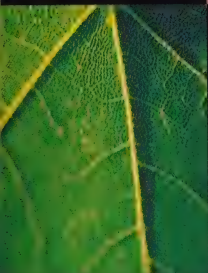
CA1  
ND800  
-S16



Government  
Publications

COMMUNICATIONS  
SECURITY  
ESTABLISHMENT  
COMMISSIONER

# Annual Report



2005-2006

Canada



Office of the Communications Security Establishment Commissioner  
P.O. Box 1984  
Station "B"  
Ottawa, Ontario  
K1P 5R5

Tel.: (613) 992-3044  
Fax: (613) 992-4096  
Website: <http://csec-ccst.gc.ca>

© Minister of Public Works and Government Services Canada 2006  
ISBN 0-662-49258-7  
Cat. No. D95-2006

Communications Security  
Establishment Commissioner



The Right Honourable Antonio Lamer,  
P.C., C.C., C.D., LL.D., D.U.

Commissaire du Centre de la  
sécurité des télécommunications

Le très honorable Antonio Lamer,  
c.p., C.C., c.d., LL.D., d.u.

April 2006

Minister of National Defence  
4Gen G.R. Pearkes Building, 13th Floor  
101 Colonel By Drive, North Tower  
Ottawa, Ontario  
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63 (3) of the *National Defence Act*, I am pleased  
to submit to you my 2005–2006 annual report on my activities and findings, for your submission  
to Parliament.

Yours sincerely,

Antonio Lamer



## TABLE OF CONTENTS

the Commissioner's Role .....	1
the Review Environment .....	3
• Three-year review of the Anti-Terrorism Act .....	3
• "Whistle-blower" legislation .....	4
• Bills that died on the order paper .....	4
• The Arar Commission .....	6
• Interception of private communications by the U.S. National Security Agency .....	7
the Year in Review .....	8
• Review activities and highlights .....	8
• Workplan .....	8
• Methodology .....	8
• Reviews undertaken .....	9
• Legal interpretations .....	9
• Review highlights .....	10
• 2005–2006 findings .....	11
• Complaints about CSE activities .....	12
• Duties under the Security of Information Act .....	12
the Impact of Review .....	12
the Commissioner's Office .....	14
Looking to the Future .....	15
• Internationally .....	15
• At home .....	15
in Closing .....	17
Annex A: Mandate of the Communications Security Establishment Commissioner .....	19
Annex B: Classified Reports, 1996–2006 .....	21
Annex C: Statement of Expenditures, 2005–2006 .....	25
Annex D: History of the Office of the Communications Security Establishment Commissioner (OCSEC) .....	27





## THE COMMISSIONER'S ROLE

Parliament passed the *Anti-Terrorism Act* in December 2001. This amended the *National Defence Act (NDA)* and established in legislation the role and responsibilities of the Communications Security Establishment (CSE) and the CSE Commissioner.

My primary legislated duty is to review the activities of CSE to determine whether they comply with the laws of Canada. The Act charges me to review CSE's activities in general and, as well, specifically to review activities that CSE carries out under ministerial authorization. Given the nature of CSE's activities, I place a particular emphasis on determining whether those activities are carried out in a manner that appropriately protects the privacy of Canadians,<sup>1</sup> as CSE is required to do by law.

My other duties include undertaking such investigations as I consider necessary in response to any complaints received about CSE's activities, and informing the Minister of National Defence and the Attorney General of Canada about any CSE activity that I believe may not be in compliance with the law.

As I see it, my main role as the CSE Commissioner is to give assurance to the Minister of National Defence that the intrusive powers Parliament granted to CSE are used in accordance with the legislation. Annex A of this report sets out the key elements of my mandate under the *National Defence Act*, as well as my duties under the *Security of Information Act*.

The Communications Security Establishment, the subject of my attention as Commissioner, is a central player in Canada's security and intelligence community. CSE's mandate under Part V.1 of the *National Defence Act* includes:

- acquiring and using information from the global information infrastructure to provide the

---

<sup>1</sup> It is important to note that "Canadians" includes Canadian citizens, permanent residents and corporations incorporated in Canada.

---

Government of Canada with foreign intelligence in accordance with the government's intelligence priorities;

- helping to protect electronic information and information infrastructures that are of importance to the Government of Canada; and
- providing technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

I carry out all my responsibilities in full recognition of the importance of CSE's contribution to ensuring that the Government of Canada is in a position to play an active, well-informed role in promoting and protecting Canadian interests in a rapidly changing world. In light of the continuing threat of terrorism around the world in recent years, I am particularly aware of CSE's important contribution to protecting the security of Canada and Canadians. It is not my intention to impede CSE from fulfilling its important role. Rather, I believe that CSE's effectiveness is enhanced when I am able to provide evidence-based assurance not only about the lawfulness of its activities, but also about the policies, procedures and processes it has in place to help ensure that lawfulness.

I am pleased to submit this annual report summarizing my office's activities and findings for the year ended 31 March 2006. In doing so, I would like to express my appreciation for the cooperation and assistance that my office received from the CSE's new Chief and his staff throughout the year. Although it is normal, and indeed fitting, for a measure of healthy tension to exist in the relationship between any review body and the organization being reviewed, the professionalism of CSE's employees

---

<sup>2</sup> Foreign intelligence is defined in Part V.1 of the *NDA* as "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security".

has facilitated the work of my office and made it more productive.

## THE REVIEW ENVIRONMENT

### Three-year review of the Anti-Terrorism Act

Several developments during the year, some of them new and some of them continuing, have the potential to shape the security and intelligence sector in general, as well as the roles and responsibilities of review bodies such as my office. I have monitored these developments closely and seized the opportunity to contribute to them as appropriate.

The omnibus *Anti-Terrorism Act* resulted in key amendments to several existing Acts, including amendments to the *National Defence Act* that provided the legislative basis for CSE as well as the CSE Commissioner. The *Anti-Terrorism Act* required a review of its provisions and operation within three years of receiving Royal Assent, and the Special Senate Committee on the *Anti-Terrorism Act* was created for this purpose in December 2004.

I appeared before the Special Senate Committee on 13 June 2005, as well as the House of Commons Sub-Committee on Public Safety and National Security two days later, on 15 June. On both occasions, I set out my views on the legislation, based on the experience of this office since its enactment. In my remarks, I made it very clear that the legislation itself is absolutely essential. However, I noted also that fine-tuning and clarification of some of its provisions — particularly those relating to ministerial authorizations to intercept private communications for the purpose of obtaining foreign intelligence<sup>3</sup> — would help eliminate ambiguities and ensure a common understanding of the operational application of these provisions. In

---

<sup>3</sup> In my 2004–2005 Annual Report, I outlined my views in some detail on how I have interpreted and will continue to discharge my mandate in respect of foreign intelligence ministerial authorizations (pp. 7–10).

---

addition to my appearances, I wrote to the Chair of the Sub-Committee to provide my views on certain recommendations made by other witnesses that would affect my office.

Upon the dissolution of Parliament in November 2005, the Special Senate Committee on the *Anti-Terrorism Act* was also dissolved without having issued its report. The new Parliament was not yet in session when my reporting period ended on 31 March 2006, but I will monitor future developments in this area with keen interest.

## **“Whistle-blower” legislation**

The *Public Servants Disclosure Protection Act* (the so-called “whistle-blower” legislation) received Royal Assent in November 2005. The Act establishes procedures for the disclosure of wrongdoings in the public sector and provides for the protection of persons who disclose the wrongdoings. Although my office will be subject to this Act, the Communications Security Establishment is excluded from the definition of “public sector” and thus from its general application. However, the Act provides that excluded organizations, such as CSE, must establish similar procedures, specific to the organization concerned.

The Act has yet to come into effect, and I understand that Bill C-2 (*Federal Accountability Act*) tabled by the new government may change some of the provisions of the “whistle-blower” legislation. Nevertheless, it is probable that CSE will be required to establish procedures for the disclosure of wrongdoings, including the protection of persons who disclose them — with a possible review role for the CSE Commissioner. I am quite prepared to take on responsibilities in this regard if called upon to do so.

## **Bills that died on the order paper**

Two proposed pieces of legislation with the potential to influence the environment within which my office carries out its work died on the order paper when Parliament was dissolved in November 2005. As of



the end of this reporting period, the new government had not yet announced whether either initiative will be pursued.

Bill C-74 (*Modernization of Investigative Techniques Act*) received first reading in the House of Commons in November 2005. The Bill would require telecommunications service providers to put in place and maintain capabilities that facilitate the lawful interception of information transmitted by telecommunications, and to provide basic information about their subscribers to specified authorities.

The proposed legislation would not affect CSE's mandate in relation to foreign intelligence or its mandate to protect electronic information and information infrastructures. It could, however, influence the extent of the technical and operational assistance CSE provides to federal law enforcement and security agencies in the performance of their lawful duties.

Bill C-81 (*An Act to establish a National Security Committee of Parliamentarians*) also received first reading in the House of Commons in November 2005. The mandate of the proposed committee would be to review the legislative, regulatory, policy and administrative framework for national security, and the activities of federal departments and agencies relating to national security. It is not intended, however, to duplicate the work of existing review bodies.

I would welcome the prospect of Parliament playing a more active role in security and intelligence matters, including scrutiny of the work of review bodies such as my office. However, I also recognize some challenges in this regard. These include, for example, the composition of the committee and its access to classified information and documents.

## The Arar Commission

The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, chaired by Mr. Justice Dennis O'Connor, was established in February 2004. Among other things, the Commission is mandated to recommend a review mechanism for the activities of the Royal Canadian Mounted Police (RCMP) with respect to their national security activities. In relation to this part of its mandate, the Commission examined intelligence review models in Canada and internationally, and held public consultations. My office contributed both written and oral submissions. My basic message to the Commission was that the model already in place for reviewing Canada's security and intelligence agencies is a good one, and experience shows that it works.

The key characteristics of the model include separate review agencies, with each review agency having:

- a mandate aligned specifically to the functions and activities of the agency reviewed;
- full independence;
- broad, unfettered access to facilities, personnel and information;
- authority to review all operational activities as well as to investigate complaints; and
- the responsibility to report to the minister accountable to Parliament for the agency under review, so that accountability to Parliament is clear and uncompromised.

The strengths of the model, therefore, include appropriateness, effectiveness and accountability. Moreover, the model's flexibility means that it can be readily adapted to particular circumstances and requirements, including a mechanism uniquely suited to reviewing the RCMP's national security activities.

## Interception of private communications by the U.S. National Security Agency

I look forward with interest to the Commission's report and its recommendations.

In late 2005, the United States media reported that following the events of 11 September 2001, President George W. Bush ordered the National Security Agency (NSA), in the interests of national security, to intercept private communications of Americans without a court warrant. In doing so, according to press reports, the President bypassed the process established for such circumstances under the *Foreign Intelligence Surveillance Act* of 1978.

Understandably, questions, commentary and speculation began to appear in the Canadian media about CSE's role and activities in the current threat environment. As a result, I made my own extensive inquiries that included discussions and communications with the Chief, CSE and drew on the considerable body of work carried out by my office in recent years. It is not my intention to comment in any way on the lawfulness of the NSA's activities, as they are well beyond my purview. However, I have decided to take the opportunity afforded me by this Annual Report to highlight the regime in place in Canada.

Part V.1 of the *National Defence Act* allows CSE to collect communications, even if they enter or exit Canada, provided that the target for the collection is a foreign entity located outside of Canada. In other words, the target cannot be a Canadian or located geographically in Canada. This kind of collection, where the end not targeted is in Canada, must be authorized by the Minister of National Defence in advance of the collection. The *NDA* sets out conditions that must be met to the Minister's satisfaction in order for a ministerial authorization to be issued. It was Parliament's view that a ministerial authorization, entrenched in legislation, provides a better approach to establishing the required authority

than a court warrant, as the latter would have no application to foreign targets located outside Canada.

The regime in place for CSE to acquire communications of foreign entities, even if a communication originates in or enters Canada (and is thus a private communication<sup>4</sup>), is based in legislation. Further, the *NDA* requires me, as the CSE Commissioner, to review CSE activities to ensure that they comply with the law. It directs me specifically to review activities carried out under a ministerial authorization to ensure they were authorized, and to report annually to the Minister on my review. A summary of my review work completed in the year ended 31 March 2006 follows.

## THE YEAR IN REVIEW

### Review activities and highlights

#### Workplan

A regularly updated three-year workplan guides my office's review program. This plan, which I approve, is driven in part by my staff's extensive knowledge of CSE's activities. It gives priority to reviewing those activities where the risks to the privacy of Canadians are believed highest.

#### Methodology

My staff has access to all the CSE premises, documents, files and personnel required to carry out reviews. They conduct thorough file and document reviews, interview CSE officials and carry out a variety of checks and tests to determine whether CSE has carried out its activities lawfully and has appropriately protected the privacy of Canadians. It is important to note that these reviews are normally carried out after the fact, in order not to intervene, without cause, in CSE's activities and operations while they are being conducted.

---

<sup>4</sup> The *Criminal Code* definition of a private communication includes any communication that originates or terminates in Canada made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended.



When a review is completed, I provide a classified report to the Minister of National Defence.<sup>5</sup> Each report provides the Minister with my opinion on the lawfulness of the activities reviewed and includes any recommendations that I consider to be appropriate in the circumstances. Such recommendations generally address shortcomings in CSE's policies, procedures or practices that, if not corrected, increase the risk that unlawful activity might occur. In this, as in so many other cases, I am firmly convinced that an ounce of prevention is worth a pound of cure.

### **Reviews undertaken**

In 2005–2006, my office completed a total of seven reviews. Six reviews were of CSE activities carried out under ministerial authorization. One of these six dealt with foreign intelligence collection, and five involved information technology security (ITS) operations. I also submitted a classified report to the Minister on a subject related to my general mandate to review the activities of CSE to ensure they are in compliance with the law. None of my seven reviews of CSE activities completed in 2005–2006 reported unlawful conduct.

### **Legal interpretations**

With respect to my reviews of CSE activities carried out under ministerial authorization, I note that I concluded on their lawfulness in light of the Department of Justice interpretation of the applicable legislative provisions. I have pointed out elsewhere that there are ambiguities in the legislation as now drafted, a view that I share with my predecessor, the Hon. Claude Bisson, O.C., a former Chief Justice of Quebec. Currently, two eminent lawyers, the Deputy

---

<sup>5</sup> Annex B lists all classified reports produced by the CSE Commissioner since 1996, when this office was established.



---

Minister of Justice and my independent Legal Counsel disagree over the meaning of key provisions that influence the nature of the assurance that I can provide. This underlines the importance of seizing the next opportunity to make statutory amendments.

### **Review highlights**

Findings from my recent reviews of foreign intelligence collection under ministerial authorization have drawn my attention to the process CSE uses to translate approved government intelligence priorities into targeting specific foreign entities. I believe it should be possible to identify a clear linkage between the government intelligence priorities, the foreign entities targeted and the activity or class of activities for which ministerial authorization is needed.

However, reviews completed by my office, including the most recent one, have shown that supporting documentation provided by CSE as part of requests for the Minister's authorization address the underlying foreign intelligence requirements only in general terms. The lack of clarity in this regard has made it difficult for my staff to assess compliance with certain of the conditions that the legislation requires to be satisfied before a ministerial authorization is given. I have offered specific recommendations to the Minister and CSE for strengthening the process.

I provided a single integrated report to the Minister on the five reviews of ITS activities carried out by CSE under ministerial authorizations. As in previous reports, I set out in this report my continuing concern with CSE's record-keeping practices. I recognize that CSE is taking steps to improve its corporate records management practices in general. The authority to intrude on the privacy of Canadians in the course of protecting the government's computer systems and networks under an ITS ministerial authorization is a sensitive matter. CSE has acknowledged its

---

responsibility to be able to record and account for such intrusions. I believe that CSE ought to give prompt attention to improving record-keeping practices in this regard, and I have asked my staff to monitor this issue closely in future reviews.

Under my general mandate to review the activities of CSE to ensure they comply with the law, I examined CSE's foreign intelligence collection activities directed at countering the threat posed by the proliferation of weapons of mass destruction and their delivery systems. Following the terrorist attacks in the U.S. in 2001, CSE enhanced its activities in the counter-proliferation area. It sends reports, based on the intelligence it collects and analyses, to Government of Canada clients and to allied agencies.

In June 2005 I provided the Minister with a classified report setting out the findings of this review. The CSE activities I reviewed complied with the law. The review identified, however, areas of policy weakness and, in one instance, a need to reconcile policy and practice. CSE accepted my recommendations, though in some cases with modifications, which they explained to me.

## **2005–2006 findings**

In accordance with well-established practice, in each Annual Report I summarize my findings about the lawfulness of CSE's activities based on the reviews my office has completed in the past year. I am able to report that the CSE activities examined during the period under review complied with the law as it is currently interpreted by the Department of Justice, and I am satisfied that CSE lawfully used and retained the intercepted private communications that were examined by my office in 2005–2006.

## Complaints about CSE activities

In addition to setting out my review mandate, the *National Defence Act* also requires me, in response to a complaint, to undertake any investigation I consider necessary to determine whether CSE engaged, or is engaging in unlawful activity. Complaints may be submitted by Canadians who believe that CSE has acted unlawfully in the performance of its duties. Until this past year, the Commissioner's office had received no complaints that required formal investigation.

There were again a limited number of complaints in 2005–2006 and, with one exception, they were not within my mandate. The one complaint received that both fell within my mandate and required investigation was still under investigation at the end of this reporting year. I anticipate that the investigation will be completed in spring 2006, after which I will report my findings to the Minister.

## Duties under the Security of Information Act

The *Security of Information Act* establishes a process that persons permanently bound to secrecy under the Act must follow if they wish to claim a “public interest” defence for divulging classified information. For classified information about CSE, the CSE Commissioner is part of the process (see Annex A). No such matters were referred to me in 2005–2006.<sup>6</sup>

## THE IMPACT OF REVIEW

The impact of review by an office such as mine may be direct or indirect. Assessing that impact is inherently difficult because, if effective, its main influence is on preventing unlawful or undesirable acts or things from happening.

Indirect impacts can result simply from the existence and mandate of a review body, and the effect these have on how the reviewed organization conducts its

---

<sup>6</sup> My website at <http://csec-ccst.gc.ca> provides an overview of my office's processes for handling complaints under the *National Defence Act* and for concerns raised pursuant to the *Security of Information Act*.

affairs. Nevertheless, my observations and discussions over the past three years make me confident that the mandate and work of my office has a positive influence on the manner in which CSE carries out its activities and on helping to ensure that they are conducted in compliance with the law.

The findings and recommendations of specific reviews have a more direct impact — particularly as a result of the action that the reviewed organization takes in response to them. When warranted by the findings, my review reports may include recommendations for action by CSE to correct deficiencies in policies, procedures or practices that increase the risk of unlawful activity. The status of recommendations is the subject of periodic discussions between my staff and CSE, and my office continues to track their disposition.

I am encouraged by CSE's positive response to the recommendations my office has made. Of almost 100 recommendations made by the CSE Commissioner since the establishment of this office, 75 percent were accepted by CSE and have either been fully implemented or are at various stages of being implemented. Half of the remaining recommendations were accepted with some modifications or are very recent and are still being considered by CSE. The remainder were either bypassed by events or, in a few cases, not accepted by CSE. Where CSE has either accepted recommendations with modifications or has rejected them, CSE officials have explained the reasons to me, with some discussions still pending.

I commend the new Chief of CSE for his ready acceptance of the importance of review, and welcome his continuing cooperation and willingness to help my office monitor the status of recommendations as an important indicator of the impact of review.

## THE COMMISSIONER'S OFFICE

In 2005–2006, my office's expenditures of \$1,043,540 were well within budget for the period. Annex C to this report provides a summary of 2005–2006 expenditures.

In carrying out my mandated responsibilities, I continue to rely on the expertise, loyalty and commitment of my staff. My office has a full-time working staff of eight people, supplemented by contracted professionals who bring a range of skills, knowledge and experience to bear as and when required.

I encourage and support several activities to help ensure that my staff continues to sharpen skills, broaden knowledge and experience, and remain fully engaged in the review community and in issues facing the security and intelligence sector in general. Such developmental opportunities in 2005–2006 included:

- initiating what has become known as the Review Agencies Forum. This involves my staff as well as the staffs of the Security Intelligence Review Committee, the Office of the Inspector General of the Canadian Security Intelligence Service and the Commission for Public Complaints Against the RCMP, who meet and share experiences, discuss issues of mutual interest and concern and identify best practices in review;
- continuing to host informal presentations to my office by government officials and academics on matters relating to security and intelligence as well as review;
- attendance of my staff at several conferences and symposia, including the 20<sup>th</sup> Anniversary International Conference of the Canadian Association for Security and Intelligence Studies; an International Symposium on Making National Security Accountable; the National Security



Studies Seminar of the Canadian Forces College;  
and the 4<sup>th</sup> Annual Charter Conference of the  
Ontario Bar Association.

In 2004–2005, my staff began the practice of giving presentations to new CSE employees — as part of their orientation course — about the duties, powers and work of the CSE Commissioner. These presentations continued in 2005–2006. I believe that this is an excellent way for my office to participate in assuring that CSE employees are aware of the Commissioner's mandate as well as how this mandate is discharged in practice.

## LOOKING TO THE FUTURE

### Internationally

Since assuming my responsibilities as the CSE Commissioner almost three years ago, terrorism has continued to be a dominant issue on the international political and security scene. Since my last report, the global war on terrorism has continued unabated. There have been numerous attacks around the globe, including the bombings in London, England in July 2005 and the subsequent arrest of alleged terrorists. International concerns have also increased sharply over the proliferation of weapons of mass destruction, with a particular focus on North Korea and the nuclear ambitions and intentions of Iran.

In Afghanistan, Canada accepted a lead role in providing security and helping to re-build the area in and around Kandahar. This undertaking has been made all the more important and dangerous with Osama bin Laden's exhortation to his extremist followers to prepare for a protracted war with the West.

### At home

In Canada, terrorism, the proliferation of weapons of mass destruction and military deployments are not our only concerns. Canada is an integral part of an economically interdependent world and must

---

continue both to protect and promote its national interests in that context.

With no foreseeable diminution in perceived threats to the security of Canada and Canadians, or of the need to provide the Government of Canada with the foreign intelligence it requires to pursue and to protect Canada's interests around the world, CSE's role will continue to be important. By extension, I believe that the work of my office in reviewing CSE's activities, in assessing their compliance with the law, and in making recommendations to ensure that such compliance is based on sound policies, procedures and practices, has a useful role to play.

Many government initiatives and activities do not fit neatly into the artificial construct of a particular fiscal year. As a result, there are several matters that will carry forward, and that I hope to see completed or otherwise resolved early in 2006–2007. These include, for example, the three-year review of the *Anti-Terrorism Act*, the Bills that died on the order paper when the 38<sup>th</sup> Parliament was dissolved, and the report of the Arar Commission, as discussed earlier in this report.

In terms of the work of my office, a major, two-phased review of CSE's activities in support of the RCMP is nearing completion. My 2004–2005 Annual Report included a general outline of the Phase 1 findings and recommendations. I am hopeful that outstanding issues arising from the Phase 2 work will be expeditiously resolved, and I plan to report the Phase 2 findings and recommendations to the Minister early in 2006–2007.

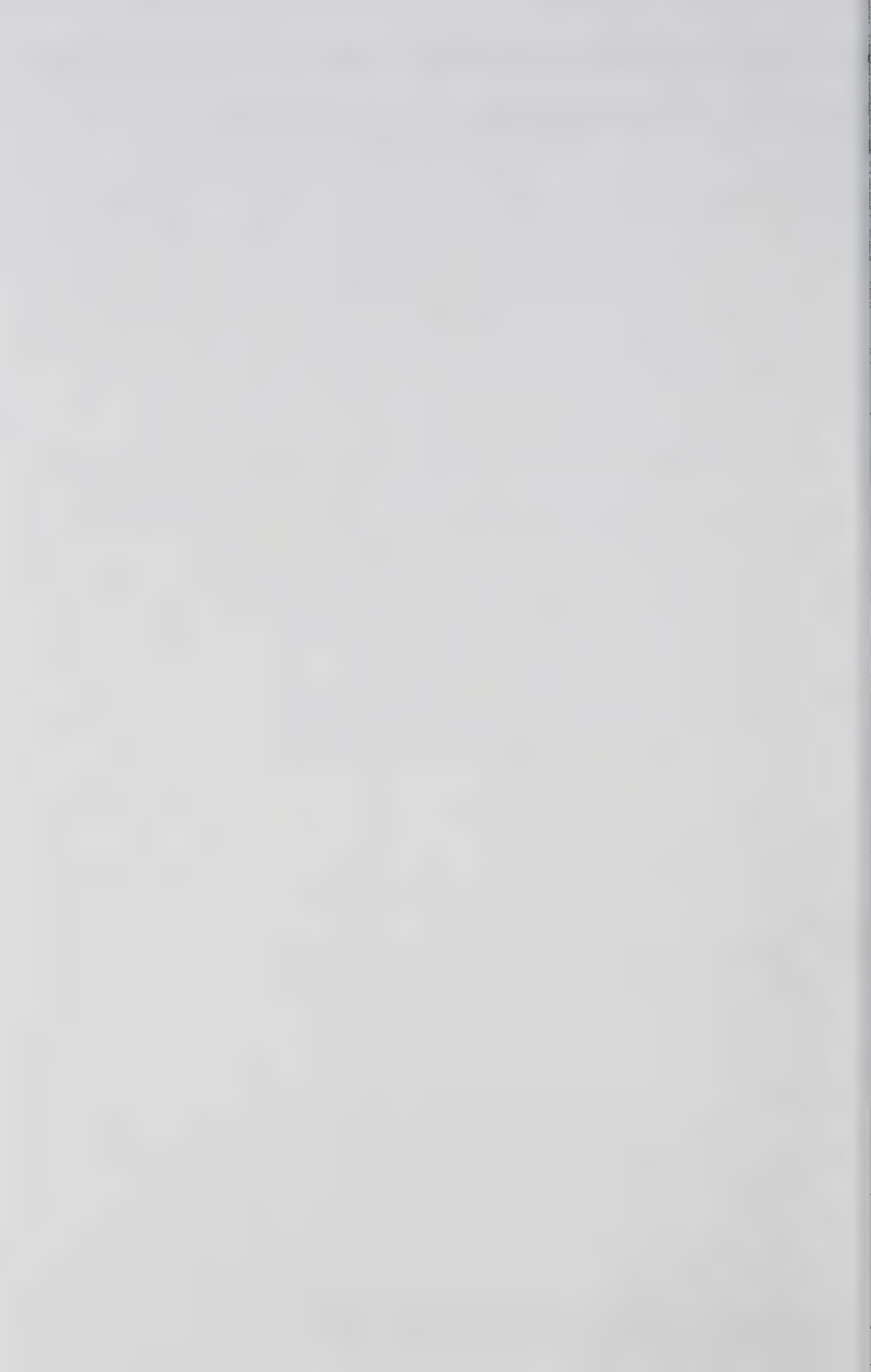
Finally, to ensure that the watcher is indeed watched, I have recently commissioned two independent management reviews of my own office. One will focus on administration, including the management and control of financial, human and information

---

resources. The other will deal with operations, by assessing whether the office carries out the Commissioner's mandated responsibilities efficiently and effectively. The reviews will address those aspects of administration and operations that pose potential risks for this office and that are important to get right. As such, I expect that they will provide evidence-based assurance in relation to some matters, as well as recommendations for action where improvements are necessary. Both reviews are scheduled to be completed in summer 2006.

## IN CLOSING

My term expires on 19 June 2006. As a result, this is my last report as CSE Commissioner. I must say that I am extremely grateful for the opportunity I have had to serve Canada, this country that I love, in a capacity that has brought its challenges, but that I have found to be rewarding in so many different ways. My one regret will be if I leave this position without a resolution of the legal interpretation issues that have bedevilled this office since December 2001. If that does indeed turn out to be the case, I wish my successor well in bringing this matter to a satisfactory conclusion for all concerned.



## Mandate of the Communications Security Establishment Commissioner

### *National Defence Act – Part V.1*

- 73.63** (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.
- (2) The duties of the Commissioner are
- (a) to review the activities of the Establishment to ensure that they are in compliance with the law;
  - (b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and
  - (c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.
- (3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.
- (4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.
- (5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.
- (6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.



- (7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

- 273.65** (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

*Security of Information Act*

- 15.** (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]
- (5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]
- (b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]
- (ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

## Classified Reports, 1996–2006

1. Classified Report to the Minister  
– March 3, 1997 (TOP SECRET)
2. Classified Report to the Minister  
– Operational policies with lawfulness implications – February 6, 1998  
(SECRET)
3. Classified Report to the Minister  
– CSE’s activities under \*\*\* – March 5, 1998 (TOP SECRET Codeword/CEO)
4. Classified Report to the Minister  
– Internal investigations and complaints – March 10, 1998 (SECRET)
5. Classified Report to the Minister  
– CSE’s activities under \*\*\* – December 10, 1998 (TOP SECRET/CEO)
6. Classified Report to the Minister  
– On controlling communications security (COMSEC) material – May 6, 1999  
(TOP SECRET)
7. Classified Report to the Minister  
– How we test (A classified report on the testing of CSE’s signals intelligence collection and holding practices, and an assessment of the organization’s efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)
8. Classified Report to the Minister  
– A study of the \*\*\* collection program – November 19, 1999 (TOP SECRET Codeword/CEO)
9. Classified Report to the Minister  
– On \*\*\* – December 8, 1999 (TOP SECRET/COMINT)
10. Classified Report to the Minister  
– A study of CSE’s \*\*\* reporting process — an overview (Phase I) – December 8, 1999 (SECRET/CEO)
11. Classified Report to the Minister  
– A study of selection and \*\*\* — an overview – May 10, 2000  
(TOP SECRET/CEO)

12. Classified Report to the Minister
  - CSE’s operational support activities under \*\*\* — follow-up – May 10, 2000 (TOP SECRET/CEO)
13. Classified Report to the Minister
  - Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)
14. Classified Report to the Minister
  - On findings of an external review of CSE’s ITS program – June 15, 2000 (SECRET)
15. Classified Report to the Minister
  - CSE’s policy system review – September 13, 2000 (TOP SECRET/CEO)
16. Classified Report to the Minister
  - A study of the \*\*\* reporting process — \*\*\* (Phase II) – April 6, 2001 (SECRET/CEO)
17. Classified Report to the Minister
  - A study of the \*\*\* reporting process — \*\*\* (Phase III) – April 6, 2001 (SECRET/CEO)
18. Classified Report to the Minister
  - CSE’s participation \*\*\* – August 20, 2001 (TOP SECRET/CEO)
19. Classified Report to the Minister
  - CSE’s support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – August 20, 2001 (TOP SECRET/CEO)
20. Classified Report to the Minister
  - A study of the formal agreements in place between CSE and various external parties in respect of CSE’s Information Technology Security (ITS) – August 21, 2002 (SECRET)
21. Classified Report to the Minister
  - CSE’s support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – November 13, 2002 (TOP SECRET/CEO)
22. Classified Report to the Minister
  - CSE’s \*\*\* activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)

23. Classified Report to the Minister
  - Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)
24. Classified Report to the Minister
  - CSE’s activities pursuant to \*\*\* Ministerial authorizations including \*\*\*
  - May 20, 2003 (SECRET)
25. Classified Report to the Minister
  - CSE’s support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part I
  - November 6, 2003 (TOP SECRET/COMINT/CEO)
26. Classified Report to the Minister
  - CSE’s support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part II
  - March 15, 2004 (TOP SECRET/COMINT/CEO)
27. Classified Report to the Minister
  - A review of CSE’s activities conducted under \*\*\* Ministerial authorization
  - March 19, 2004 (SECRET/CEO)
28. Classified Report to the Minister
  - Internal investigations and complaints — follow-up – March 25, 2004 (TOP SECRET/CEO)
29. Classified Report to the Minister
  - A review of CSE’s activities conducted under 2002 \*\*\* Ministerial authorization – April 19, 2004 (SECRET/CEO)
30. Classified Report to the Minister
  - Review of CSE \*\*\* operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)
31. Classified Report to the Minister
  - CSE’s support to \*\*\* – January 7, 2005 (TOP SECRET/COMINT/CEO)
32. Classified Report to the Minister
  - External review of CSE’s \*\*\* activities conducted under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)
33. Classified Report to the Minister
  - A study of the \*\*\* collection program – March 15, 2005 (TOP SECRET/COMINT/CEO)

- 
34. Classified Report to the Minister
    - Report on the activities of CSE's \*\*\* – June 22, 2005 (TOP SECRET)
  35. Classified Report to the Minister
    - Interim report on CSE's \*\*\* operations conducted under Ministerial authorization – March 2, 2006 (TOP SECRET/COMINT)
  36. Classified Report to the Minister
    - External review of CSE \*\*\* activities conducted under Ministerial authorization – March 29, 2006 (TOP SECRET/CEO)



---

## Statement of Expenditures 2005–2006

### Standard Object Summary

Salaries and Wages	\$527,760
Transportation and Telecommunications	16,655
Information	24,177
Professional and Special Services	321,484
Rentals	132,326
Purchased Repair and Maintenance	426
Materials and Supplies	7,155
Acquisition of Machinery and Equipment	9,591
Other Expenditures	3,966
<b>Total</b>	<b>\$1,043,540</b>



---

## History of the Office of the Communications Security Establishment Commissioner (OCSEC)

The Office of the Communications Security Establishment Commissioner was created on June 19, 1996, with the appointment of the inaugural Commissioner, The Honourable Claude Bisson, O.C., a former Chief Justice of Quebec, who held the position until June 2003. He was succeeded by the Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., Chief Justice of Canada (retired) for a term of three years.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act*. During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment (CSE) to determine whether they conformed with the laws of Canada; and to receive complaints about CSE's activities.

Following the terrorist attacks in the United States on September 11, 2001, Parliament adopted the omnibus *Anti-Terrorism Act* which came into force on December 24, 2001. The omnibus Act introduced amendments to the *National Defence Act*, by adding Part V.1 and creating legislative frameworks for both OCSEC and CSE. It also gave the Commissioner new responsibilities to review activities carried out by CSE under a ministerial authorization.

The omnibus legislation also introduced the *Security of Information Act* that replaced the *Official Secrets Act*. This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSE on the grounds that it is in the public interest.

Under the Commissioner's current mandate, which entrenched in law the original mandate established in 1996 as well as the additional responsibilities described above, the Commissioner has retained the powers of a commissioner under Part II of the *Inquiries Act*.

## Historique du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST)

Le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) a été créé le 19 juin 1996, au moment de la nomination du premier commissaire, l'honorable Claude Bissson, O.C., ancien juge en chef du Québec. M. Bissson a occupé le poste de commissaire jusqu'en juin 2003. Le très honorable Antonio Lamer, c.p., C.C., c.d., LL.D., d.u., juge en chef du Canada (à la retraite), lui a alors succédé pour un mandat de trois ans.

Pendant les six premières années de son mandat (de juin 1996 à décembre 2001), le commissaire a exercé ses fonctions conformément à plusieurs décrets, pris en vertu de la partie II de la *Loi sur les enquêtes*. Au cours de cette période, il a assumé une double responsabilité : examiner les activités du Centre de la sécurité des télécommunications (CST) afin de déterminer si elles étaient en conformité avec les lois du Canada, et recevoir les plaintes relatives aux activités du CST.

Dans le sillage des attentats terroristes du 11 septembre 2001, le Parlement a adopté la *Loi antiterroriste* omnibus, qui a été promulguée le 24 décembre 2001. Cette loi modifie la *Loi sur la défense nationale*, en y ajoutant la partie V.1, qui établit le cadre législatif du BCCST et du CST, et elle confie au commissaire de nouvelles responsabilités relatives à l'examen des activités que mène le CST sous le régime d'une autorisation ministérielle.

En outre, la *Loi omnibus* a remplacé la *Loi sur les secrets officiels* par la *Loi sur la protection de l'information*, laquelle attribue au commissaire des fonctions précises pour les cas où une personne astreinte au secret à perpétuité souhaiterait invoquer la défense de l'intérêt public pour justifier la divulgation de renseignements classifiés sur le CST.

En vertu de son mandat actuel, qui inscrit dans la loi le mandat initial établi en 1996 ainsi que les nouvelles responsabilités supplémentaires décrites ci-dessus, le commissaire conserve tous les pouvoirs que confère à un commissaire la partie II de la *Loi sur les enquêtes*.





## État des dépenses, 2005-2006

### Sommaire des articles courants

Traitements et salaires	527 760 \$
Transports et télécommunications	16 655
Information	24 177
Services professionnels et spéciaux	321 484
Location	132 326
Achat de services de réparation et d'entretien	426
Fournitures et approvisionnements	7 155
Acquisition de machines et de matériel	9 591
Autres charges	3 966
<b>Total</b>	<b>1 043 540 \$</b>

32. Classified Report to the Minister  
– External review of CSE's \*\*\* activities conducted under Ministerial authorization – 28 février 2005 (TRÈS SECRET/COMINT/Réservé aux Canadiens)
33. Classified Report to the Minister  
– A study of the \*\*\* collection program – 15 mars 2005 (TRÈS SECRET/COMINT/Réservé aux Canadiens)
34. Classified Report to the Minister  
– Report on the activities of CSE's \*\*\* – 22 juin 2005 (TRÈS SECRET)
35. Classified Report to the Minister  
– Interim report on CSE's \*\*\* operations conducted under Ministerial authorization – 2 mars 2006 (TRÈS SECRET/COMINT)
36. Classified Report to the Minister  
– External review of CSE's \*\*\* activities conducted under Ministerial authorization – 29 mars 2006 (TRÈS SECRET/Réservé aux Canadiens)

22. Classified Report to the Minister  
– CSE's \*\*\* activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization – 27 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)
23. Classified Report to the Minister  
– Lexicon of CSE definitions – 26 mars 2003 (TRÈS SECRET)
24. Classified Report to the Minister  
– CSE's activities pursuant to \*\*\* Ministerial authorizations including \*\*\*  
– 20 mai 2003 (SECRET)
25. Classified Report to the Minister  
– CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part I – 6 novembre 2003 (TRÈS SECRET/COMINT/Réservé aux Canadiens)
26. Classified Report to the Minister  
– CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part II – 15 mars 2004 (TRÈS SECRET/COMINT/Réservé aux Canadiens)
27. Classified Report to the Minister  
– A review of CSE's activities conducted under \*\*\* Ministerial authorization – 19 mars 2004 (SECRET/Réservé aux Canadiens)
28. Classified Report to the Minister  
– Internal investigations and complaints — follow-up – 25 mars 2004 (TRÈS SECRET/Réservé aux Canadiens)
29. Classified Report to the Minister  
– A review of CSE's activities conducted under 2002 \*\*\* Ministerial authorization – 19 avril 2004 (SECRET/Réservé aux Canadiens)
30. Classified Report to the Minister  
– Review of CSE \*\*\* operations under Ministerial authorization – 1<sup>er</sup> juin 2004 (TRÈS SECRET/COMINT)
31. Classified Report to the Minister  
– CSE's support to \*\*\* – 7 janvier 2005 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

12. Classified Report to the Minister  
– CSE's operational support activities under \*\*\* — follow-up – 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)
13. Classified Report to the Minister  
– Internal investigations and complaints — follow-up – 10 mai 2000 (SECRET)
14. Classified Report to the Minister  
– On findings of an external review of CSE's ITS program – 15 juin 2000 (SECRET)
15. Classified Report to the Minister  
– CSE's policy system review – 13 septembre 2000 (TRÈS SECRET/Réservé aux Canadiens)
16. Classified Report to the Minister  
– A study of the \*\*\* reporting process — \*\*\* (Phase II) – 6 avril 2001 (SECRET/Réservé aux Canadiens)
17. Classified Report to the Minister  
– A study of the \*\*\* reporting process — \*\*\* (Phase III) – 6 avril 2001 (SECRET/Réservé aux Canadiens)
18. Classified Report to the Minister  
– CSE's participation \*\*\* – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)
19. Classified Report to the Minister  
– CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)
20. Classified Report to the Minister  
– A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – 21 août 2002 (SECRET)
21. Classified Report to the Minister  
– CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – 13 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

## Rapports classifiés de 1996 à 2006

1. Classified Report to the Minister  
– 3 mars 1997 (TRÈS SECRET)
2. Classified Report to the Minister  
– Operational policies with lawfulness implications – 6 février 1998 (SECRET)
3. Classified Report to the Minister  
– CSE's activities under \*\*\* – 5 mars 1998 (TRÈS SECRET Mot codé/Réservé aux Canadiens)
4. Classified Report to the Minister  
– Internal investigations and complaints – 10 mars 1998 (SECRET)
5. Classified Report to the Minister  
– CSE's activities under \*\*\* – 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)
6. Classified Report to the Minister  
– On controlling communications security (COMSEC) material – 6 mai 1999 (TRÈS SECRET)
7. Classified Report to the Minister  
– How we test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) – 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)
8. Classified Report to the Minister  
– A study of the \*\*\* collection program – 19 novembre 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)
9. Classified Report to the Minister  
– On \*\*\* – 8 décembre 1999 (TRÈS SECRET/COMINT)
10. Classified Report to the Minister  
– A study of CSE's \*\*\* reporting process – an overview (Phase I) – 8 décembre 1999 (SECRET/Réservé aux Canadiens)
11. Classified Report to the Minister  
– A study of selection and \*\*\* – an overview – 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)



[...]

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

**273.65** (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.

### *Loi sur la protection de l'information*

**15.** (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]

(5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]

b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession : [...]

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.

273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

- a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;
- b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;
- c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.



## CONCLUSION

caractéristique importante. Je prévois que ces études nous donneront l'assurance, prouvées à l'appui, que nous sommes sur la bonne voie et feront des recommandations si des améliorations sont nécessaires. Cet exercice devrait se terminer à l'été 2006.

Mon mandat prend fin le 19 juin 2006. Le présent rapport est donc le dernier que je signerai en qualité de commissaire du CST. Je suis extrêmement heureux de la possibilité qui m'a été offerte de servir ce grand pays qu'est le Canada dans une fonction qui comportait certes une bonne part de défis, mais qui m'a aussi apporté de nombreuses satisfactions. Mon seul regret serait peut-être de devoir quitter mon poste avant qu'aient pu se régler les problèmes d'interprétation juridique qui compromettent la bonne marche des activités de ce bureau depuis décembre 2001. Si tel devait être le cas, je souhaite à mon successeur tout le succès possible, pour toutes les parties concernées, dans la conclusion de ce dossier.

recommandations pour faire en sorte que cette légalité repose sur des politiques, des procédures et des pratiques solides, mon bureau accomplit une œuvre utile.

Bon nombre des initiatives et des activités gouvernementales ne s'inscrivent pas aussi naturellement que l'on le souhaiterait dans la structure artificielle que représente un exercice financier. Par conséquent, plusieurs dossiers doivent être reportés à l'exercice suivant. Parmi ceux que je souhaite voir menés à bien ou réglés au début de 2006-2007, mentionnons l'examen triennal de la *Loi antiterroriste*, les projets de loi morts au Feuilleton au moment de la dissolution du 38<sup>e</sup> Parlement et le rapport de la Commission Arar dont j'ai déjà discuté plus haut.

Pour ce qui est des travaux de mon bureau, un examen de première importance, réalisé en deux temps, concernant les activités du CST à l'appui de la GRC sera bientôt terminé. Mon rapport annuel pour 2004-2005 donne un aperçu des conclusions et des recommandations relatives à la première phase. J'espère que les points laissés en suspens dans la seconde seront réglés sans tarder, et je compte soumettre au ministre mes conclusions et mes recommandations relatives à la deuxième phase au début de 2006-2007.

Enfin, pour que le contrôleur que je suis fasse lui aussi l'objet de certaines vérifications, j'ai récemment demandé deux examens indépendants de la gestion de mon propre bureau. L'un portera sur le volet administratif, notamment la gestion et le contrôle des ressources financières, humaines et de l'information. L'autre se concentrera sur les opérations et visera à établir dans quelle mesure nous nous acquittons avec efficacité et efficience des responsabilités prévues dans le mandat du commissaire. Les deux études traiteront des aspects qui présentent une part de risques pour le Bureau et pour lesquels l'exacitude représente une



Depuis mon entrée en fonction à titre de commissaire du CST, il y a presque trois ans, le terrorisme a continué de dominer la scène de l'actualité politique et de la sécurité internationales. Après le dépôt de mon dernier rapport, la guerre mondiale contre le terrorisme s'est poursuivie avec une égale intensité. Les attentats se sont multipliés partout sur la planète, comme à Londres, en juillet 2005, suivis par l'arrestation de terroristes présumés. La prolifération des armes de destruction massive suscite une inquiétude croissante partout dans le monde, particulièrement face à la Corée du Nord et aux ambitions et aux intentions de l'Iran en matière nucléaire.

En Afghanistan, le Canada a accepté de jouer un rôle de premier plan dans le maintien de la sécurité ainsi que dans les travaux de reconstruction à Kandahar et dans les environs. L'importance de cette mission, et les dangers qu'elle recèle, a été renforcée par les exhortations à une guerre prolongée contre l'Occident lancées par Oussama Ben Laden à ses disciples extrémistes.

Au Canada, nos préoccupations ne se limitent pas au terrorisme, à la prolifération des armes de destruction massive et au déploiement de soldats canadiens. En effet, le Canada fait partie intégrante d'une économie mondiale interdépendante et il doit continuer de protéger et de promouvoir ses intérêts nationaux.

Comme on ne peut pas s'attendre, dans un avenir prévisible, à une diminution des menaces potentielles à la sécurité du Canada et de sa population, ou de la nécessité de fournir au gouvernement du Canada les renseignements étrangers dont il a besoin pour promouvoir et défendre les intérêts du pays dans le monde, le rôle du CST demeurera important. Au-delà, j'estime qu'en examinant les activités du CST pour en contrôler la légalité et en formulant des

En 2004-2005, mon personnel a commencé à présenter des exposés aux nouveaux employés du CST – dans le cadre de leur cours d'initiation – concernant les responsabilités, les pouvoirs et les fonctions du commissaire du Centre de la sécurité des télécommunications. Ces exposés se sont poursuivis en 2005-2006. À mon avis, ils offrent à mon bureau un excellent moyen de contribuer à informer les employés du CST du mandat du commissaire et de la façon dont il est mis en œuvre.

- de l'Ontario.

Charte organisée par l'Association du Barreau canadiennes et la 4<sup>e</sup> conférence annuelle sur la études de sécurité nationale du Collège des Forces en matière de sécurité nationale, le Séminaire des le colloque international sur la responsabilisation pour l'étude de la sécurité et du renseignement, 20<sup>e</sup> anniversaire de l'Association canadienne la conférence internationale soulignant le à plusieurs conférences et symposiums, dont

la présence des membres de mon personnel
- renseignement ainsi que les examens;

des questions touchant la sécurité et le

des hauts fonctionnaires et des universitaires sur

des présentations informelles dans nos locaux par

exemplaires en matière d'examen;

préoccupations d'intérêt mutuel et des pratiques

discuter de leur expériences, de questions et de

des plaintes du public contre la GRC, pour

renseignement de sécurité et de la Commission

de l'inspecteur général du Service canadien du

activités de renseignement de sécurité, du Bureau

recommandations ont perdu leur pertinence par suite des événements ou, dans un petit nombre de cas, ont été rejetées par le CST. Chaque fois que mes recommandations ont été modifiées ou rejetées, des représentants du CST m'ont fait part de leurs raisons et, dans certains cas, les discussions se poursuivent.

Je félicite le nouveau chef du CST, qui a rapidement reconnu l'importance de l'examen, et me réjouis de son esprit de coopération et de l'aide qu'il apporte aux membres de mon personnel dans le suivi de nos recommandations, et que je considère comme un important indicateur des répercussions de l'examen.

En 2005-2006, les dépenses de mon bureau se sont chiffrées à 1 043 540 \$ et ont été largement couvertes par le budget approuvé pour cette période. On en trouvera un résumé à l'annexe C.

Dans l'exercice des responsabilités énoncées dans mon mandat, je continue de m'appuyer sur le savoir-faire, la loyauté et l'engagement des membres de mon personnel. Mon bureau dispose d'un effectif de huit employés à plein temps, auquel peuvent venir s'ajouter des spécialistes engagés à contrat qui nous font bénéficier au besoin de leurs compétences, de leurs connaissances et de leur expérience.

J'encourage et appuie diverses activités qui aident mon personnel à continuer de perfectionner ses compétences, d'élargir ses connaissances et son expérience et de maintenir un engagement entier à l'égard du milieu des organismes d'examen et des enjeux auxquels fait face le secteur de la sécurité et du renseignement en général. Pour 2005-2006, je citerai notamment les activités suivantes :

- la création d'une instance connue aujourd'hui sous le nom de Tribune des organismes d'examen, qui réunit mon personnel ainsi que les membres du personnel du Comité de surveillance des

## LE BUREAU DU COMMISSAIRE

Les examens effectués par un bureau comme le mien peuvent avoir des répercussions directes ou indirectes. Ces répercussions sont en soi difficiles à évaluer, car si l'organisme est efficace, elles ont pour conséquence principale de prévenir des actes illicites ou indésirables.

Les effets indirects peuvent résulter simplement de l'existence et du mandat d'un organisme d'examen, qui ont une influence sur la manière dont l'organisme visé par l'examen mène ses activités. Cela dit, à la lumière de mes observations et des discussions que j'ai eues au cours des trois dernières années, je suis persuadé que le mandat et les travaux de mon bureau ont une influence positive sur la façon dont le CST exerce ses activités et l'aident à les mener dans le respect de la loi.

Les conclusions et recommandations d'examens en particulier ont des répercussions plus directes, principalement en raison des mesures que l'organisme visé doit prendre pour y donner suite. Lorsque les circonstances le justifient, il arrive que je recommande au CST des moyens de combler certaines lacunes touchant des politiques, des procédures ou des pratiques, qui augmentent le risque d'activités illicites. La suite donnée à mes recommandations fait l'objet de discussions périodiques entre mon personnel et celui du CST, et nous suivons de près les progrès accomplis.

Je suis encouragé par l'accueil favorable qu'ont reçu nos recommandations. Depuis la création du Bureau, le commissaire du CST a présenté près d'une centaine de recommandations. De ce nombre, près de 75 p. 100 ont été acceptées par le CST et mises en œuvre intégralement ou en partie ou sont en voie d'être mises en œuvre. La moitié des autres recommandations ont été légèrement reformulées avant d'être acceptées, ou sont trop récentes et sont encore à l'étude au sein du CST. Pour le reste, les



## Plaintes relatives aux activités du CST

En plus de délimiter mon mandat concernant les examens, la *Loi sur la défense nationale* prévoit que, si des plaintes sont déposées, je dois y donner suite en procédant à toutes les enquêtes que je juge nécessaires, afin de déterminer si le CST s'est engagé dans des activités illicites ou s'il est en voie de le faire. Les plaintes peuvent être déposées par des Canadiens qui estiment que le CST a enfreint la loi dans l'exercice de ses fonctions. Jusqu'à l'an passé, le Bureau du commissaire n'avait reçu aucune plainte nécessitant une enquête formelle.

Un nombre limité de plaintes ont été déposées en 2005-2006, qui, à une exception près, ne relevaient pas de mes compétences. Celle qui relevait de mon mandat et qui nécessitait la tenue d'une enquête, n'avait pas encore été réglée à la fin de la période de référence. Je prévois que l'enquête prendra fin au printemps 2006, après quoi je rendrai compte de mes conclusions au ministre.

## Fonctions exercées en vertu de la Loi sur la protection de l'information

La *Loi sur la protection de l'information* fixe la procédure que doivent suivre les personnes assujetties, de par la *Loi*, au secret à perpétuité, qui souhaitent se prévaloir de la « défense d'intérêt public » pour divulguer des renseignements classifiés. Dans le cas de l'information classifiée touchant le CST, le commissaire a un rôle à jouer (voir l'annexe A). Aucun problème de ce genre ne m'a été soumis en 2005-2006.

<sup>6</sup> Mon site Web, à l'adresse <http://csec-ccst.gc.ca>, présente un survol des méthodes qu'utilise mon bureau dans le cas de plaintes déposées en vertu de la *Loi sur la protection de l'information*.



## Constatations en 2005-2006

crois qu'il doit s'occuper sans tarder de perfectionner ses méthodes en matière de gestion des dossiers, et j'ai demandé à mon personnel de suivre attentivement cette question dans les examens à venir.

Dans le cadre de mon mandat général concernant la légalité des activités du CST, j'ai examiné les activités de collecte de renseignements étrangers visant à contrer la menace que présente la prolifération d'armes de destruction massive et de leurs modes de livraison. Au lendemain des attentats terroristes de 2001 aux États-Unis, le CST a dû renforcer ses activités de contre-prolifération. Il envoie des rapports, fondés sur les renseignements qu'il a obtenus et analysés, à ses clients du gouvernement du Canada et aux services de pays alliés.

En juin 2005, j'ai remis au ministre un rapport classifié dans lequel je rends compte de cet examen. Les activités du CST que j'ai examinées sont conformes à la loi. Mes travaux ont toutefois fait ressortir certains points faibles sur le plan stratégique et, dans un cas particulier, la nécessité de concilier les politiques et les pratiques. Le CST a accepté mes recommandations, sous réserve, dans certains cas, de modifications dont on m'a expliqué les raisons.

Conformément à une pratique bien établie, je procède dans chaque rapport à un résumé de mes conclusions quant à la légalité des activités du CST, à la lumière des examens effectués au cours de l'exercice. Je suis en mesure de rapporter que les activités examinées au cours de l'exercice satisfont aux dispositions de la loi et à l'interprétation qu'en donne pour l'instant le ministère de la Justice. Je puis aussi affirmer que le CST a utilisé et conservé dans les limites prescrites par la loi les communications privées qu'il a interceptées et que j'ai examinées durant l'exercice 2005-2006.

## Points saillants de l'examen

Les constatations de mes derniers examens concernant la collecte de renseignements étrangers sous le régime d'une autorisation ministérielle ont attiré mon attention sur la façon dont le CST utilise les priorités du gouvernement en matière de renseignements pour cibler certaines entités étrangères. À mon avis, il devrait être possible d'établir un lien clair entre ces priorités, les entités ciblées et l'activité ou la catégorie d'activités nécessitant l'autorisation du ministre.

Or, les examens effectués par mon bureau, y compris le plus récent, ont montré que la documentation accompagnant les demandes d'autorisation ministérielle du CST ne traite des priorités sous-jacentes du gouvernement en matière de renseignements étranger que de façon générale. En raison de ce manque de clarté, il a été difficile à mon personnel d'établir si certaines conditions obligatoires pour la délivrance d'une autorisation ministérielle avaient été respectées. J'ai soumis au ministre ainsi qu'au CST des recommandations précises en vue de renforcer ce processus.

J'ai regroupé dans un seul rapport au ministre le compte rendu des cinq examens dont ont fait l'objet les opérations du CST axées sur la STI et menées sous le régime d'une autorisation ministérielle. Comme par le passé, j'y ai fait valoir les préoccupations que continuent de susciter les pratiques du CST au chapitre de la tenue des dossiers. Je reconnais que le CST prend des mesures pour améliorer en général ses méthodes à cet égard. Le pouvoir de s'immiscer dans les affaires privées des Canadiens dans le cadre d'activités effectuées en vertu d'une autorisation ministérielle axée sur la STI, afin de protéger les réseaux et systèmes informatiques du gouvernement, est une question épineuse. Le CST a reconnu qu'il doit pouvoir consigner ces intrusions et en rendre compte. Je

## Examens effectués

En 2005-2006, mon bureau a effectué au total sept examens. Six d'entre eux portaient sur des activités exercées par le CST sous le régime des autorisations ministérielles; dans un cas, il s'agissait de collecte de renseignements étrangers et dans les cinq autres, d'activités axées sur la sécurité des technologies de l'information (STI). J'ai également remis au ministre un rapport classifié qui portait sur l'un des aspects de mon mandat général relatif à la légalité des activités du CST. Aucun des sept examens menés au cours de l'exercice n'a révélé de conduite illicite de la part du CST.

## Interprétation juridique

Pour établir la légalité des activités exercées par le CST en vertu d'autorisations ministérielles, je tiens compte de l'interprétation que le ministère de la Justice donne des dispositions applicables de la loi. Comme je l'ai déjà souligné, ces dispositions législatives, dans leur version actuelle, comportent des ambiguïtés, ce que croyait aussi mon prédécesseur, l'honorable Claude Bisson, O.C., ancien juge en chef du Québec. Pour le moment, deux éminents avocats, le sous-ministre de la Justice et ma conseillère juridique indépendante, ne s'entendent pas sur l'interprétation à donner des principales dispositions, ce qui influence le type d'assurance que je peux fournir. C'est pourquoi il est important de saisir la prochaine occasion qui se présentera d'apporter des modifications législatives.

politiques, les procédures ou les pratiques du CST, qui, si elles ne sont pas corrigées, augmentent le risque d'activités illicites. Comme c'est souvent le cas, ici ou ailleurs, je suis fermement convaincu qu'il vaut mieux prévenir que guérir.

Plan de travail

de présenter au ministre, une fois par an, les conclusions de mon enquête. Un résumé de mes travaux d'examen au cours de l'exercice terminé le 31 mars 2006 est présenté ci-après.

Un plan de travail triennal, mis à jour régulièrement, guide le programme d'examen de mon bureau. Ce plan, qui doit recevoir mon approbation, repose en partie sur la connaissance détaillée des activités du CST que possèdent les membres de mon personnel. Il accorde la plus haute importance à l'examen des activités où les risques pour la vie privée des Canadiens sont jugés les plus élevés.

Méthodologie

Mon personnel a accès à l'ensemble des locaux, des documents, des dossiers et du personnel que requiert l'examen des activités du CST. Celui-ci prend des formes diverses : étude approfondie des dossiers et des documents; entretiens avec les employés du CST; vérifications de toutes sortes permettant d'établir si l'organisme s'est acquitté de son mandat dans le respect de la loi et s'il a protégé la vie privée des Canadiens. Il convient de souligner que ces examens sont habituellement réalisés après le fait, afin d'éviter toute intervention sans mérite dans le déroulement des activités et opérations du CST.

Lorsqu'un examen est terminé, j'en rends compte au ministre de la Défense nationale<sup>5</sup> dans un rapport classifié, dans lequel je donne mon opinion sur la légalité des activités en question et je formule les recommandations qui m'apparaissent pertinentes dans les circonstances. Ces recommandations portent généralement sur des lacunes dans les

<sup>5</sup> L'annexe B donne une liste des rapports classifiés que le commissaire du Centre de la sécurité des télécommunications a produits depuis la création de son bureau, en 1996.

dernières années. Il n'est pas question pour moi de commenter la légalité des activités de la NSA, puisqu'elles ne sont pas de mon ressort. Par contre, j'ai décidé de profiter de l'occasion que m'offre le présent rapport annuel pour mettre en lumière le régime en place au Canada.

La partie V.1 de la *Loi sur la défense nationale* permet au CST de collecter des communications, y compris des communications à destination ou en provenance du Canada, pour autant que la cible soit une entité étrangère située à l'extérieur du Canada. Autrement dit, la cible ne peut pas être un Canadien ni être située au Canada. Ce type de collecte dans lequel la partie non ciblée se trouve au Canada doit être autorisé, au préalable, par le ministre de la Défense nationale. La *LDN* fixe les conditions qui doivent être remplies à la satisfaction du ministre pour que celui-ci délivre une autorisation ministérielle. Le Parlement était d'avis qu'une autorisation ministérielle, prévue par la loi, constituait une meilleure approche pour conférer le pouvoir requis que le recours à un mandat, lequel ne pourrait pas s'appliquer à des cibles étrangères situées à l'extérieur du Canada.

Le régime qui permet au CST d'intercepter les communications d'entités étrangères, même s'il s'agit de communications en provenance ou à destination du Canada (c'est-à-dire des communications privées<sup>4</sup>), est prescrit par la loi. Par ailleurs, la *LDN* me charge, en tant que commissaire du CST, d'examiner les activités de l'organisme pour en contrôler la conformité. Elle stipule plus précisément que je suis tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation ministérielle, afin de garantir qu'elles ont bel et bien été autorisées, et

<sup>4</sup> Aux termes du *Code criminel*, une communication privée s'entend de toute communication en provenance ou à destination du Canada, où son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers.



- une entière indépendance;

- un accès large et sans entrave aux installations,

au personnel et à l'information;

- le pouvoir d'examiner toutes les activités opérationnelles et de faire enquête sur les plaintes;
- l'obligation de rendre compte au ministre

responsable devant le Parlement de l'organisme soumis à un examen, de sorte que la reddition de comptes au Parlement soit claire et rigoureuse.

Les points forts du mécanisme sont donc la pertinence, l'efficacité et la reddition de comptes. Sa souplesse permet en outre de l'adapter facilement à des circonstances et des exigences particulières, et de prévoir par exemple un mécanisme visant uniquement à examiner les activités de la GRC en matière de sécurité nationale.

J'attends avec intérêt le rapport de la Commission et ses recommandations.

À la fin de 2005, les médias américains ont rapporté qu'après les attentats du 11 septembre 2001, le président George W. Bush avait ordonné à la National Security Agency (NSA), dans l'intérêt de la sécurité nationale, d'intercepter sans mandat des communications privées de citoyens américains. Selon la presse, par ces mesures, le président outrepassait le processus établi pour de telles circonstances dans la *Foreign Intelligence Surveillance Act* de 1978.

Naturellement, des questions, des commentaires et des hypothèses ont commencé à paraître dans les médias canadiens concernant le rôle et les activités du CST dans le contexte de menace actuel. J'ai donc fait des recherches approfondies – j'ai notamment discuté et échangé de l'information avec le chef du CST – et j'ai fait appel à la somme considérable des travaux effectués par mon personnel au cours des

## Interception de communications privées par la National Security Agency des États-Unis

## Commission Arar

des communes en novembre 2005. Le comité proposé aurait pour mandat d'examiner les cadres législatif, réglementaire, stratégique et administratif de la sécurité nationale, ainsi que les activités des ministères et organismes fédéraux responsables de la sécurité nationale. Il ne devrait toutefois pas faire double emploi avec les activités des organismes d'examen en place.

Je conviens que le Parlement pourrait jouer un rôle plus actif dans les questions relatives à la sécurité et au renseignement, y compris l'examen des travaux des organismes d'examen tels que celui dont je suis responsable. Cependant, je suis conscient de certains défis que cela suppose, notamment la composition du comité et son accès à des renseignements et à des documents classifiés.

La Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, présidée par le juge Dennis O'Connor, a été mise sur pied en février 2004. Elle est chargée entre autres de recommander un mécanisme d'examen concernant les activités de la Gendarmerie royale du Canada (GRC) relatives à la sécurité nationale. Dans le cadre de cette partie de son mandat, la Commission a considéré des mécanismes canadiens et étrangers d'examen dans le domaine du renseignement et a tenu des consultations publiques. Mon bureau a soumis des observations écrites et orales. Mon principal message à la Commission était que le mécanisme canadien en place est efficace et que l'expérience a prouvé qu'il fonctionne bien.

Les principaux éléments du mécanisme prévoient des organismes d'examen distincts ayant chacun :

- un mandat propre aux fonctions et aux activités de l'organisme examiné;

La Loi n'est pas encore en vigueur, et il semble que le projet de loi C-2 (*Loi fédérale sur l'imputabilité*) déposé par le nouveau gouvernement puisse en modifier certaines dispositions. Il est néanmoins probable que le CST devra se doter de procédures concernant la divulgation des actes répréhensibles – et la protection des divulgateurs –, conférant probablement un rôle d'examinateur au commissaire du CST. Le cas échéant, je suis tout à fait prêt à assumer cette responsabilité.

Deux projets de loi pouvant influencer sur le contexte dans lequel mon bureau exerce ses activités sont morts au Feuilleton lorsque le Parlement a été dissout en novembre 2005. À la fin de la période de référence, le nouveau gouvernement n'avait pas encore indiqué s'il donnerait suite à ces projets de loi.

Le projet de loi C-74 (*Loi sur la modernisation des techniques d'enquête*) a fait l'objet d'une première lecture à la Chambre des communes en novembre 2005. Il obligerait les fournisseurs de services de télécommunications à prendre les dispositions nécessaires pour faciliter l'interception licite de l'information transmise par télécommunication et à fournir des renseignements de base sur leurs abonnés aux autorités mentionnées. Ce projet de loi n'aurait aucune incidence sur le mandat du CST concernant la fourniture de renseignements étrangers ou la protection des renseignements électroniques et des infrastructures d'information. Toutefois, il pourrait influencer sur la portée de l'aide technique et opérationnelle que le CST transmet aux organismes fédéraux d'application de la loi et de sécurité dans l'exercice des fonctions que la loi leur confère.

Le projet de loi C-81 (*Loi constituant le Comité de parlementaires sur la sécurité nationale*) a également été lu pour la première fois à la Chambre

*Loi* est absolument indispensable, certaines de ses dispositions devraient être précisées et explicitées – notamment celles touchant les autorisations ministérielles permettant l'interception de communications privées en vue d'obtenir des renseignements étrangers<sup>3</sup> – afin d'éliminer les ambiguïtés et d'assurer une compréhension commune de l'application opérationnelle de ces dispositions. En outre, j'ai écrit au président du Sous-comité pour lui faire part de mon opinion au sujet de certaines recommandations formulées par d'autres témoins, qui pourraient avoir une incidence sur mon bureau.

Après la dissolution du Parlement en

novembre 2005, le Comité spécial du Sénat sur la *Loi antiterroriste* a également été dissout

sans avoir déposé son rapport. Le 31 mars 2006, à la fin de la période de référence, le nouveau

Parlement n'avait pas encore commencé à siéger, mais je suivrai les faits nouveaux dans ce domaine

avec un grand intérêt.

*La Loi sur la protection des fonctionnaires*

*divulgateurs d'actes répréhensibles* (aussi appelée « loi sur les divulgateurs ») a reçu la sanction royale en novembre 2005. La *Loi* prévoit des procédures de divulgation des actes fautifs dans le secteur public et renferme des dispositions sur la protection des divulgateurs. Quoique mon bureau soit assujéti à cette loi, le CST est exclu de la définition de « secteur public » et, par conséquent, de l'application générale de la *Loi*. Toutefois, cette dernière prévoit que les organisations exclues, tel le CST, doivent mettre en place des procédures similaires propres à leur organisme.

<sup>3</sup> Dans mon rapport annuel 2004-2005, j'ai présenté mon point de vue concernant la façon dont j'ai interprété et continuerais de remplir mon mandat relatif aux autorisations ministérielles en matière de renseignement étranger (p. 8-11).



C'est avec plaisir que je dépose ce rapport annuel, qui résume les activités et les constatations de mon bureau pour l'exercice terminé le 31 mars 2006. J'en profite pour souligner la façon dont le nouveau chef du CST et son personnel ont coopéré avec les membres de mon personnel tout au long de l'année et les ont appuyés. S'il est normal, et même indiqué, qu'une saine tension existe dans une certaine mesure entre l'organisme d'examen et l'organisme examiné, le professionnalisme des employés du CST a facilité le travail de mon personnel et l'a rendu plus productif.

Plusieurs faits nouveaux survenus au cours de l'année et l'évolution de certains dossiers en cours pourraient avoir une incidence sur le secteur de la sécurité et du renseignement en général, ainsi que sur les rôles et les responsabilités des organismes d'examen comme celui dont je suis responsable. J'ai surveillé de près ces développements et j'ai profité, au besoin, de l'occasion pour y contribuer.

## CONTEXTE DE L'EXAMEN

### Examen triennal de la Loi antiterroriste

La *Loi antiterroriste* omnibus a apporté des modifications importantes à plusieurs lois en vigueur, notamment la *Loi sur la défense nationale*, qui énonce le fondement législatif du CST et du poste de commissaire du CST. La *Loi antiterroriste* prévoit la tenue d'un examen de ses dispositions et de son application trois ans après l'obtention de la sanction royale; c'est pour cette raison que le Comité spécial du Sénat sur la *Loi antiterroriste* a été mis sur pied en décembre 2004.

J'ai comparu devant le Comité spécial du Sénat le 13 juin 2005, ainsi que devant le Sous-comité de la sécurité publique et nationale de la Chambre des communes deux jours plus tard, soit le 15 juin. Dans les deux cas, j'ai présenté mon point de vue sur la législation, à partir de l'expérience de mon bureau depuis sa mise en application. Dans mes observations, j'ai indiqué très clairement que, si la



<sup>2</sup> Le renseignement étranger est défini à la partie V.1 de la *Loi sur la défense nationale* : renseignements sur les moyens, les intentions ou les activités d'un étranger, d'un État étranger, d'une organisation étrangère ou d'un groupe terroriste étranger et qui portent sur les affaires internationales, la défense ou la sécurité.

J'exerce toutes mes responsabilités en reconnaissant pleinement l'importante contribution du CST pour faire en sorte que le gouvernement du Canada puisse jouer un rôle actif et bien informé dans la défense et la protection des intérêts canadiens dans un monde en rapide évolution. Compte tenu de la menace terroriste qui a persisté partout dans le monde au cours des dernières années, je suis particulièrement conscient du rôle important que joue le CST pour protéger la sécurité des Canadiens et de leur pays. Je n'ai nullement l'intention d'empêcher le CST de s'acquitter de cette importante fonction, mais je crois que l'organisme gagne en efficacité si je peux affirmer, preuves à l'appui, non seulement qu'il exerce ses activités en toute légalité, mais aussi que les politiques, procédures et processus qu'il a mis en place aident à garantir cette légalité.

mandat du CST, énoncé à la partie V.1 de la *Loi sur la défense nationale*, est le suivant :

- acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers<sup>2</sup>, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
- fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;
- fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère.

Le Parlement a adopté en décembre 2001 la *Loi antiterroriste*, qui modifiait la *Loi sur la défense nationale* (LDN) et stipulait le rôle et les responsabilités du Centre de la sécurité des télécommunications (CST) et de son commissaire.

Ma principale responsabilité aux termes de la loi consiste à examiner les activités du CST pour en contrôler la légalité. Je suis chargé d'examiner les activités du CST en général et, en particulier, celles qu'il exerce en vertu d'autorisations ministérielles. Étant donné la nature des activités de l'organisme, j'attache une importance particulière à vérifier s'il a exercé ces activités de manière à protéger adéquatement la vie privée des Canadiens<sup>1</sup> comme il est tenu de le faire en vertu de la loi.

Mes autres fonctions consistent à effectuer les enquêtes que je juge nécessaires en raison de plaintes reçues au sujet des activités du CST, et à informer le ministre de la Défense nationale et le procureur général du Canada dans tous les cas où l'organisme pourrait ne pas avoir agi en conformité avec la loi.

J'estime que ma principale attribution à titre de commissaire du CST est de donner au ministre de la Défense nationale l'assurance que le CST a utilisé les pouvoirs d'intrusion que lui confère le Parlement, sans enfreindre la loi. Les éléments clés de mon mandat en vertu de la *Loi sur la défense nationale*, ainsi que mes responsabilités en vertu de la *Loi sur la protection de l'information* sont présentés à l'annexe A.

Le Centre de la sécurité des télécommunications, sur lequel se porte mon attention en tant que commissaire, joue un rôle central dans le domaine de la sécurité et du renseignement canadiens. Le

<sup>1</sup> Il convient de noter que le terme « Canadiens » englobe les citoyens, les résidents permanents et les sociétés du Canada.



# TABLE DES MATIÈRES

1	Rôle du commissaire
3	Contexte de l'examen
3	Examen triennal de la Loi antiterroriste
4	Loi sur les divulgateurs
5	Projets de loi morts au Feuilleton
6	Commission Arar
7	Interception de communications privées par la National Security Agency des États-Unis
9	Rétrospective de l'année
9	• Activités d'examen et faits saillants
9	• Plan de travail
9	• Méthodologie
10	• Examens effectués
10	• Interprétation juridique
11	• Points saillants de l'examen
12	• Constatations en 2005-2006
13	• Plaintes relatives aux activités du CST
13	• Fonctions exercées en vertu de la Loi sur la protection de l'information
13	Répercussions de l'examen
15	Le Bureau du commissaire
17	Regard sur l'avenir
17	• Sur la scène internationale
17	• Au pays
19	Conclusion
21	Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications
23	Annexe B : Rapports classifiés de 1996 à 2006
27	Annexe C : État des dépenses, 2005-2006
29	Annexe D : Historique du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST)





2005-2006



# Rapport annuel

COMMISSAIRE  
DU CENTRE  
DE LA SÉCURITÉ  
DES TÉLÉCOMMUNICATIONS



CA1  
ND800  
-S16



COMMUNICATIONS  
SECURITY  
ESTABLISHMENT  
COMMISSIONER

# Annual Report



2006-2007

Office of the Communications Security  
Establishment Commissioner  
P.O. Box 1984  
Station "B"  
Ottawa, Ontario  
K1P 5R5

Tel.: (613) 992-3044  
Fax: (613) 992-4096  
Website: <http://csec-ccst.gc.ca>

© Minister of Public Works and  
Government Services Canada 2007  
ISBN 978-0-662-69804-3  
Cat. No. D95-2007

Communications Security  
Establishment Commissioner



The Honourable Charles D. Gonthier, Q.C.

Commissaire du Centre de la  
sécurité des télécommunications

L'honorable Charles D. Gonthier, c.r.

May 2007

Minister of National Defence  
MGen G.R. Pearkes Building, 13<sup>th</sup> Floor  
101 Colonel By Drive, North Tower  
Ottawa, Ontario  
K1A 0K2



Dear Sir:

Pursuant to subsection 273.63 (3) of the *National Defence Act*, I am pleased to submit to you my 2006–2007 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Charles D. Gonthier





---

# TABLE OF CONTENTS

Introduction /1

The Review Environment /2

- Legal interpretations /2
- Legislation lagging behind technological advances /4
- Three-year review of the *Anti-Terrorism Act* /4
- Senate Special Committee recommendations /5
- House of Commons Subcommittee recommendations /7
- The O'Connor Commission of Inquiry /8

The Year in Review /10

- Independent reviews of OCSEC /10
- Workplan /10
- Reviews undertaken of CSE /11

2006-2007 Review Highlights /12

- Review of CSE's foreign intelligence collection in support of the RCMP /12
  - Background /12
  - Methodology /12
  - Findings /13
- Review of information technology security activities at a government department /14
  - Background /14
  - Methodology /15
  - Findings /15
- Review of the roles of CSE's client relations officers and the Operational Policy Section in the release of personal information /16
  - Background /16
  - Methodology /17
  - Findings /17

---

## 2006-2007 Review Highlights (*Continued*)

- Review of CSE signals intelligence collection activities conducted under ministerial authorizations /18
  - Background /18
  - Methodology /19
  - Findings /19
- Overview of 2006-2007 findings /19
- Reviews underway/future reporting /20
- Complaints about CSE activities /20
- Duties under the *Security of Information Act* /20

## The Commissioner's Office /21

## Looking to the Future /22

- The Major Commission of Inquiry and the Iacobucci Internal Inquiry /22
- Review methodology /23

## In Closing /23

## Annex A: Mandate of the Communications Security Establishment Commissioner /25

## Annex B: Classified Reports, 1996–2007 /27

## Annex C: Statement of Expenditures, 2006-2007 /31

## Annex D: History of the Office of the Communications Security Establishment Commissioner /33

## Annex E: Role and Mandate of the Communications Security Establishment /35

# INTRODUCTION

This is my first report as Communications Security Establishment (CSE) Commissioner, since my appointment effective August 1, 2006. I have a three-year mandate that expires in August 2009.

My own background includes 30 years' experience on the bench, most recently as a Supreme Court Justice from 1989-2003. I believe there are strong parallels between the role of a judge and that of the CSE Commissioner. A judge's fundamental concern is to ensure fair trials and protect personal liberty, while maintaining peace and security. Correspondingly, the CSE Commissioner's fundamental concern is to balance the right to privacy with the need for information to protect national security. The similarity between these roles is reflected in the legislation specifying that the Commissioner be a supernumerary judge or a retired judge of a superior court.

*The CSE Commissioner's fundamental concern is to balance the right to privacy with the need for information to protect national security.*

There is, however, an important difference in context. While secrecy issues do arise in court proceedings in certain instances, for the most part the judicial process takes place in public. Secrecy, on the other hand, is at the very heart of foreign intelligence collection. Nevertheless, the balancing principles are the same. I see the role of my office as providing Canadians with the assurance that the CSE's critical intelligence work is being carefully examined by an impartial authority to ensure it is lawful, and that their rights are being protected, without compromising the secrecy required to protect national security.

In October 2006, I was presented with an exceptional opportunity to attend the International Intelligence Review Agencies Conference in Cape Town, South Africa. One of the conference themes was the need to balance the traditional rights and liberties of citizens with the need for increased powers to meet threats to national security. It was a remarkable experience to meet with the practitioners in security and intelligence review from 14 countries, including my own, and to hear from them first-hand about the challenges we all face. I remain grateful for this

opportunity because it provided an occasion for me, as the new CSE Commissioner, to become totally immersed in topics of mutual interest in the company of experts.

During the early days following my appointment, I met the Minister of National Defence and the Chief of CSE. I was also provided with extensive briefings and tours, many of them at CSE, and I am particularly grateful to my briefers for their comprehensive presentations. As time progressed, I had the opportunity to meet other federal government officials, including the Auditor General of Canada and the Privacy Commissioner, the Chairs of the Security Intelligence Review Committee and the Commission for Public Complaints Against the RCMP, the Deputy Minister of National Defence, and the National Defence Ombudsman.

Most important, of course, has been the time I have spent involving myself in the work of my office, and familiarizing myself with the activities and preoccupations of my predecessors, which will be discussed later in this report.

## THE REVIEW ENVIRONMENT

A number of key issues helped shape the environment in which this office carried out its work over the past year. Some of these have been described and commented on by my predecessors in past Annual Reports. Below, I draw attention to some themes that have not been mentioned before, as well as some new developments in ongoing issues.

### Legal interpretations

Since the omnibus *Anti-Terrorism Act* was proclaimed in December 2001, the persons who have occupied the position of CSE Commissioner have faced a persistent dilemma arising from the amendments this Act introduced to the *National Defence Act*. Particularly troublesome has been the Commissioner's duty to review the activities of CSE conducted under ministerial authorizations issued for the sole purpose of obtaining foreign intelligence, given the lack of agreement on the interpretation of key provisions of the Act.

On the one hand, my predecessors and I have recognized the importance of CSE's work, and the benefit the Government of Canada derives from the foreign intelligence CSE provides, particularly during a time when the threat of global terrorism continues unabated, and the safety of our soldiers in Afghanistan remains at risk.

On the other hand, during our respective terms as Commissioner, each of us has been unequivocal in the position that the legal interpretation and advice regarding ministerial authorizations provided to CSE by the Department of Justice is not supported by a simple reading of the appropriate provisions of Part V.1 of the *National Defence Act*, and each of us so advised the Minister of National Defence of the day. In addition, my immediate predecessor, the Right Honourable Antonio Lamer and I both made our positions known to officials at the Office of the Attorney General of Canada.

When I am asked to consider whether an activity is lawful, I must first determine what the law states in respect of that activity. The relevant Act, then, is the yardstick by which the lawfulness of the activity is measured. The difficulty arises, in instances such as this, when there is a fundamental difference of opinion about what the Act states.

I do not question the role of the Department of Justice in the drafting of legislation, nor do I view my role as Commissioner as arbiter of statutory interpretation. However, as I have informed the Minister of National Defence and the Attorney General of Canada, the legislation lacks clarity and it ought to be amended, a view I share with both my predecessors.

*The legislation lacks clarity  
and it ought to be amended.*

This matter has been under deliberation for some time, and I hope the government will make the required amendments at the earliest opportunity. I am confident that this will not be too onerous a task because other countries have successfully adopted and are applying legislation to meet similar requirements.



---

## Legislation lagging behind technological advances

As time goes on, there is an ever-widening knowledge gap between the general public and evolving technologies. In a number of respects, Canada's laws have also not kept pace with technological advances. We need a more imaginative approach. Today, criminal and terrorist elements are masters of these complex technologies and, unlike democratic institutions, are unimpeded by legal constraints. Those involved in the legislative process need to avoid laws that are driven by the technology of the day, which will in short order be superseded by new developments. Instead, we must ensure our laws have a broad enough scope, and are so structured — be it by providing for regulations or otherwise — that they can accommodate new technologies, and continue to protect both our privacy and security.

### Three-year review of the *Anti-Terrorism Act*

The *Anti-Terrorism Act* amended the *Official Secrets Act* and the *National Defence Act*, among other legislation. The amendments to the *National Defence Act* included a legislative basis for CSE and the CSE Commissioner.

The *Anti-Terrorism Act* required a review of its provisions and operation within three years of receiving royal assent, to be carried out by a designated or specially established committee of the Senate or the House of Commons, or of both chambers. A Subcommittee of the House of Commons Standing Committee on Public Safety and National Security was established for this purpose in autumn 2004. At the same time, the Senate established a Special Committee to carry out a comprehensive review of the Act. As described in the 2005-2006 Annual Report, my predecessor appeared before the Senate Special Committee on June 13, 2005, and two days later before the House of Commons Subcommittee. The Senate Special Committee reported on February 22, 2007, and the House Subcommittee reported on March 27, 2007.

## Senate Special Committee recommendations

The Senate Special Committee made several recommendations concerning CSE as well as this office. As regards CSE, the Committee focussed primarily on ministerial authorizations, stating that it accepted the explanations as to why CSE needs to intercept private communications when undertaking its foreign intelligence and information technology security activities. It also accepted Commissioner Lamer's explanation that ministerial authorizations were the proper instrument to use for intercepting private communications, rather than prior judicial authorization, because warrants from Canadian courts have no jurisdiction outside Canada.<sup>1</sup> The Committee drew comfort from the fact that this office is required to review the lawfulness of CSE's activities, including the interception of private communications under ministerial authorizations. However, it remained concerned, as was Commissioner Lamer, that the standard required to satisfy the Minister that all necessary preconditions to intercepting private communications have been met is unclear. Accordingly, the Committee recommended that subsections 273.65(2) and (4) of the *National Defence Act* be amended to clarify whether these preconditions should be based on reasonable belief or reasonable suspicion.<sup>2</sup> This has been an issue of interest to my office, and a clarification would be welcome.

*The Committee drew comfort from the fact that this office is required to review the lawfulness of CSE's activities.*

Because the Committee wished to ensure that intercepted information is disposed of if it has been determined to be non-essential or when it is no longer essential, it recommended that CSE develop information retention and disposal policies, containing specific timeframes for the disposal of intercepted information, and that it make these policies publicly available.<sup>3</sup>

<sup>1</sup> Special Senate Committee on the *Anti-Terrorism Act*, *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-Terrorism Act*, February 2007, p. 77.

<sup>2</sup> *Ibid.*, Recommendation 18, p. 78.

<sup>3</sup> *Ibid.*, Recommendation 19, p. 79.

In the interests of accountability and transparency, the Committee also recommended that the Minister of National Defence or the CSE be required to report annually to Parliament on the number of ministerial authorizations issued during the year, the number still in force by the end of the year, and the general purpose for which each authorization was issued (i.e., to obtain foreign intelligence or to protect computer systems or networks).<sup>4</sup>

The *Anti-Terrorism Act* also amended the *Official Secrets Act*, and renamed it the *Security of Information Act*, known as SOIA. SOIA establishes a process that persons permanently bound to secrecy must follow if they wish to claim a public interest defence for divulging classified information. The Commissioner may receive classified information as part of the process (see Annex A). However, the *Security of Information Act* does not describe what should be done once the Commissioner receives that information.<sup>5</sup> The Committee recommended that the Government specify the procedure to be followed in such cases.<sup>6</sup> I should point out that my office does have internal policies and procedures in place to fill the gap that the Committee identified.

Lastly, the Committee discussed the oversight and review of Canada's national security and anti-terrorism framework. The Committee mentioned that this office is "generally perceived to be an effective oversight mechanism."<sup>7</sup> The Committee recommended that a standing Senate committee be established to monitor and periodically report on Canada's anti-terrorism legislation and national security framework on an ongoing basis. In addition, the Committee called for a comprehensive parliamentary review of the provisions and operation of the *Anti-Terrorism Act* every five years.

---

<sup>4</sup> *Ibid.*, Recommendation 20, p. 79.

<sup>5</sup> To date, I have not received any information under the *Security of Information Act*.

<sup>6</sup> *Supra*, footnote 1, Recommendation 26, p. 94.

<sup>7</sup> *Supra*, footnote 1, p.116.

## House of Commons Subcommittee recommendations

The House Subcommittee's Final Report on its review of the *Anti-Terrorism Act* also addressed the issue of ministerial authorizations. In particular, I was pleased to note that the Subcommittee drew attention to the remarks of my predecessor in his 2005-2006 Annual Report about the legal ambiguities and uncertainties in the provisions allowing for ministerial authorizations, and the disagreement regarding interpretation of these provisions between this office and the Department of Justice. Without making a specific recommendation in this regard, the Subcommittee urged government counsel and me to resolve these issues as expeditiously as possible. As well, the Subcommittee requested that the Government's response to the Final Report indicate what the issues of disagreement are and how they have been resolved, to the extent possible. Failing this, the Subcommittee believes I should provide these details in my 2007-2008 Annual Report.<sup>8</sup> I intend to revisit this recommendation as the time for that report approaches.

The Subcommittee also supported a recommendation by the Privacy Commissioner that subsection 273.65(8) of the *National Defence Act* be amended to require the CSE Commissioner to review the private communication interception activities carried out under ministerial

authorization to ensure they comply with the requirements of the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*, as well as with the authorization itself. This position was reinforced with an additional recommendation that section 273.66 of the *National Defence Act* be amended to require the CSE only to undertake activities consistent with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*, in addition to the restraints on the exercise of its mandate already set out in that section.<sup>9</sup> I should point out that my office's review methodology always includes an examination of compliance with the *Charter* and the *Privacy Act*.

*My office's review methodology always includes an examination of compliance with the Charter and the Privacy Act.*

<sup>8</sup> Subcommittee on the Review of the *Anti-Terrorism Act*, *Rights, Limits, Security: A Comprehensive Review of the Anti-terrorism Act and Related Issues. Final Report of the Standing Committee on Public Safety and National Security*, March 2007, p. 56.

<sup>9</sup> *Ibid.*, Recommendations 44 and 45, pp. 55-56.



With respect to the issue of review and oversight, the Subcommittee recommended that Bill C-81 from the 38<sup>th</sup> Parliament, the proposed *National Security Committee of Parliamentarians Act*, or a variation of it, be introduced in Parliament at the earliest opportunity. The Subcommittee further recommended that the mandate of the proposed committee include undertaking compliance audits of departments and agencies, such as CSIS, CSE, and national security elements of the RCMP, in relation to the provisions of the *Anti-Terrorism Act*.<sup>10</sup> In last year's Annual Report, my predecessor welcomed the prospect of more active parliamentary review of national security activities, but also noted challenges such as the composition of the committee and its access to classified information and documents. I concur with that position in general, and intend to offer specific comments once a bill is introduced.

Finally, the Subcommittee recommended that there be another comprehensive review of the provisions and operation of the *Anti-Terrorism Act*, to begin no later than December 31, 2010, and to be completed no later than December 31, 2011. It noted that the proposed committee of parliamentarians would be well-equipped to carry out this review.<sup>11</sup>

## The O'Connor Commission of Inquiry

The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar was established February 5, 2004. It was mandated to investigate and report on the actions of Canadian officials in relation to Maher Arar (Factual Inquiry) as well as to recommend an arm's-length review mechanism for the activities of the RCMP with respect to national security (Policy Review). The Honourable Dennis O'Connor was appointed Commissioner of the Inquiry. He released his Policy Review report on December 12, 2006.

---

<sup>10</sup> *Ibid.*, Recommendations 58 and 59, pp. 84-86.

<sup>11</sup> *Ibid.*, pp. 83-85.



In order to provide integrated review of integrated national security activities, Commissioner O'Connor recommended that statutory gateways be enacted linking the proposed Independent Complaints and National Security Review Agency for the RCMP, the Security Intelligence Review Committee and the Office of the CSE Commissioner to provide for exchange of information, referral of investigations, conduct of joint investigations, and coordination and preparation of reports.<sup>12</sup> I welcome this proposal, although to date the absence of gateways has never been an operational impediment.

I was pleased to note the following observation from Justice O'Connor's report: "I am not recommending that SIRC's mandate be expanded to include the CSE, as I understand that the Office of the CSE Commissioner functions very well and I see no reason to interfere with that operation."<sup>13</sup> I was also pleased to see that my office was recognized for the creation of the Review Agencies Forum in 2005-2006.<sup>14</sup> The Forum is described further on in this report.

I do have reservations, however, regarding Justice O'Connor's recommendation to establish an Integrated National Security Review Coordinating Committee.<sup>15</sup> I am concerned that introducing such a coordinating committee by way of statute, and amendments to related legislation, may create an unnecessary and counter-productive level of bureaucracy between independent review agencies and Parliament.

---

<sup>12</sup> Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006), p. 578.

<sup>13</sup> *Ibid.*, Recommendation 11, p. 580.

<sup>14</sup> *Ibid.*, p. 282.

<sup>15</sup> *Ibid.*, Recommendation 12, p. 591.

---

## THE YEAR IN REVIEW

### Independent Reviews of OCSEC

In spring 2006, two independent management reviews of my office were commissioned. One focussed on administration, including the management and control of financial, human and information resources. The other dealt with operations, by assessing whether the office carries out the Commissioner's mandated responsibilities efficiently and effectively.

*I was pleased to note that the findings of the administrative review were all positive.*

The reports of these management reviews were available to me at the time of my appointment, thus providing me with an independent assessment

of my new area of responsibility. I was pleased to note that the findings of the administrative review were all positive. The recommendations of the operational review were discussed in detail at a review workshop held on August 21, 2006, with the review consultants as moderators. The operational review also raised methodology issues, which will be briefly referred to later in this report.

### Workplan

My office's activities are guided by a regularly updated three-year workplan. To facilitate scheduling, my staff consult with CSE about the review components of this plan. Criteria that determine their selection of topics for review include: CSE activities or programs that have not previously or recently been reviewed; areas identified from briefings requested of CSE; the status of recommendations from previous reviews; and activities where privacy is most likely to be at risk. My staff, who have extensive knowledge of CSE, ask themselves fundamental questions such as: what can go wrong; what is the probability of something going wrong; and what are the consequences if they do go wrong.

Also during the year, considerable staff time and resources were devoted to work on legal interpretation issues, which I have already described in detail above in my discussion of the review environment.

---

## Reviews undertaken of CSE

My general review mandate is set out in paragraph 273.63(2)(a) of the *National Defence Act*.<sup>16</sup> Under subsection 273.65(8) of the Act, I also have an obligation to review and report to the Minister as to whether the activities carried out under a ministerial authorization are authorized.

Ministerial authorizations for foreign intelligence collection are issued under the authority of subsection 273.65(1) of the *National Defence Act*, whereas ministerial authorizations for information technology security activities are issued under subsection 273.65(3) of the Act. Reviews of CSE's activities conducted under ministerial authorizations are undertaken only after the ministerial authorization has expired.

During 2006-2007, my office submitted classified reports of four reviews to the Minister. Two of the reviews dealt with CSE's activities conducted under ministerial authorization; one pertained to foreign intelligence collection, while the other concerned information technology security. The other two reviews were conducted under my general mandate, to ensure the activities were in compliance with the law.

---

<sup>16</sup> Please see Annex A for the text of the relevant sections of the *National Defence Act*.

---

## 2006-2007 REVIEW HIGHLIGHTS

### Review of CSE's foreign intelligence collection in support of the RCMP

#### Background

In January 2005, my office submitted a report to the Minister of National Defence examining the technical and operational assistance CSE provided to the RCMP under paragraph 273.64(1)(c) of the *National Defence Act*, also known as mandate (c).<sup>17</sup> The second and final phase of the review was completed and in June 2006, my predecessor submitted a follow-up report reviewing CSE's foreign signals intelligence collection activities in support of the RCMP under paragraph 273.64(1)(a) of the *National Defence Act*, also known as mandate (a). Further details on the first phase of the review may be obtained in the 2004-2005 Annual Report of this office.

Under mandate (a), CSE provides two kinds of foreign intelligence information to its government clients, including the RCMP. Most of its reports address general areas of interest that complement and support the client's own mandated responsibilities. In addition to this proactive support, CSE provides reactive support by responding to specific requests by the client for intelligence-related information.

#### Methodology

OCSEC staff examined CSE's mandate (a) activities in support of the RCMP for the period January 1 to December 31, 2003. They received briefings and answers to both verbal and written questions that were posed to CSE officials. They also obtained a listing of the agency's requests for intelligence-related information and chose several to examine in detail. As part of this in-depth examination, two separate demonstrations illustrating the activities under review were provided to OCSEC staff by those CSE officials who had been directly involved in responding to the requests.

---

<sup>17</sup> CSE's mandate is described in Annex E of this report.



## Findings

Many of the findings and recommendations made in my office's first report also applied to this second-phase review of assistance provided under mandate (a). For example, it was recommended CSE amend and/or update the instruments that guide its support activities to the RCMP. My predecessor was pleased to report that, for the most part, CSE had accepted these recommendations and is working to implement them.

CSE also acknowledged the need to implement a formal system of record keeping. This is a continuing concern, as was noted in my office's 2005-2006 Annual Report. CSE has advised that high priority has been given to the development and implementation of a corporate records management system that will deal with their hard-copy and electronic records requirements.

*CSE has advised that high priority has been given to the development and implementation of a corporate records management system.*

During the second phase of the review, a detailed examination of CSE's response to RCMP requests for intelligence-related information identified two issues of concern that required further legal study by CSE. The first was whether mandate (a) was the appropriate authority in all instances for CSE to provide intelligence support to the RCMP in the pursuit of its domestic criminal investigations. Pending a re-examination of this issue by CSE, no assessment was made of the lawfulness of CSE's activities in support of this agency under mandate (a) as currently interpreted and applied by CSE. My staff is monitoring the issue.

The second issue related to CSE's policies and practices as they relate to the disclosure of Canadian personal information to its clients. When collecting foreign intelligence, CSE may incidentally acquire personal information about Canadians. This information may be retained if assessed as essential to the understanding of the foreign intelligence, and it may be included in foreign intelligence reporting if it is suppressed (i.e. replaced by a generic reference such as "a Canadian person"). When receiving a subsequent request for disclosure of the full details of Canadian personal information, CSE requires its clients, including the



---

RCMP, to justify their authority to collect this information under their own respective mandates and provide an operational justification of their need to know this information. If these conditions are met, CSE releases the information.

An in-depth examination of relevant sections of the *National Defence Act* and the *Privacy Act* raised questions as to CSE's conformance with the various authorities that govern disclosure. Thus, my office recommended that CSE also re-examine its authority to collect, use and disclose personal information to certain federal government departments and agencies. In addition, my office has recommended that CSE establish agreements with client agencies to formalize the circumstances when such information may be disclosed while providing assistance under its (c) mandate.

CSE acknowledged that the report "raises a number of issues that, from a policy/legal perspective, will generate further in-depth analysis by CSE and Department of Justice legal counsel." I anticipate that this analysis will include a discussion and perhaps even a formal articulation by CSE of its position regarding the application of the *National Defence Act* as it relates to the provision of foreign intelligence in accordance with the Government of Canada intelligence priorities.

## Review of information technology security activities at a government department

### Background

This review examined information technology security activities conducted by CSE under ministerial authorization in 2004-2005 at a government department. The objective was to assess and verify compliance with the law and with the provisions of the ministerial authorization for these activities.

Individuals conducting personal and business affairs with the Government of Canada have a reasonable expectation of privacy. However, when the security of government computer systems and networks is being tested, personal information or private communications can be inadvertently intercepted with certain types of necessary testing. Subsection 273.65(3) of the *National Defence Act* provides that:

*Individuals conducting personal and business affairs with the Government of Canada have a reasonable expectation of privacy.*

The Minister may, for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the *Criminal Code*, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.

In such cases, CSE is responsible for seeking authorization on behalf of the department or agency requesting the activity to be covered. This ministerial authorization enables CSE to undertake a complete assessment of a department's computer systems and networks.

## Methodology

The review was conducted initially through examination of documents and files related to the ministerial authorization and the conditions imposed by it. Fact-finding and verification interviews were then held with CSE and selected client representatives who were identified as having direct involvement in the authorization process or ensuing activities.

## Findings

With the qualification set out below regarding one of the conditions of the ministerial authorization, this review found that CSE's work at the department was in compliance with the law and with the ministerial authorization.

The review found that the process by which CSE acquired the information technology security ministerial authorization for its activities at the department was found to be in accordance with the requirements of the *National Defence Act*. It was also determined that four of the five conditions set out in subsection 273.65(4) of the Act were complied with satisfactorily. However, with respect to one of the conditions, the review found that certain information was retained even though its retention was not essential. While CSE personnel acted in a manner that was consistent with the direction they were given, there were aspects that could be improved upon, and CSE has undertaken to do so. CSE has also indicated that future Memoranda of Understanding with client departments where information technology security activities under ministerial authorizations are to be conducted will reflect these improvements.

Other recommendations from the review included ensuring that future policy and practice promote conformance with CSE's legislated authorities as they relate to staff activities during information technology security exercises.

## **Review of the roles of CSE's client relations officers and the Operational Policy Section in the release of personal information**

### **Background**

The objective of this review was to assess the lawfulness of the activities of both the CSE client relations officers and the Operational Policy Section, as they relate to the request for and release of personal information about Canadians that has been suppressed in CSE foreign intelligence reports, as referred to previously. This information is made available to authorized Government of Canada clients, only under certain conditions.

CSE has provided foreign intelligence reports based on signals intelligence to officials in government departments since its formal establishment in 1946. Reports were delivered by hand until the creation of the on-site client relations officer programme in 1985. Client relations officers provide intelligence reports, explain to individual clients and potential

clients the role of CSE and signals intelligence, and assist in determining client needs based on Government of Canada intelligence priorities.

To protect privacy, CSE suppresses personal information about Canadians in foreign intelligence reports. If a client has both the authority and the need to know the information, it must make a formal request and provide justification. Requests for release of this information are centralized in CSE's Operational Policy Section.

*To protect privacy, CSE suppresses personal information about Canadians in foreign intelligence reports.*

The majority of requests are now made via a secure communication network directly to CSE. Client relations officers play a role in the release of Canadian identities in CSE foreign intelligence reports because they continue to deal with requests from clients who do not have access to this secure network.

## Methodology

This review examined relevant documentation, including the authorities that govern the activities of client relations officers and the CSE unit authorized to release this information. All requests for and releases of suppressed information during a six-month period were reviewed in detail to ensure compliance with law and policy. Interviews were conducted with client relations officers, their managers, and the manager of the Operational Policy Section.

## Findings

The review concluded that the activities of the CSE client relations officers and the Operational Policy Section were in compliance with the *National Defence Act* and with CSE's related policies. There were some inconsistencies in requests and releases, as well as areas where both policy and practice could be improved to enhance the protection of privacy, as required by the *Privacy Act*. Recommendations included more comprehensive training for clients who make requests, and providing more clients with secure, electronic access to CSE as a means of reducing errors and enhancing control over the process. I was pleased to note that



since the period of review there has also been increased training for and supervision of personnel in the Operational Policy Section at CSE as regards the release of suppressed information.

## Review of CSE signals intelligence collection activities conducted under ministerial authorizations

### Background

Certain foreign intelligence collection activities were conducted under three ministerial authorizations that were in effect from March 2004 to December 2006. These ministerial authorizations focused on acquiring communications of foreign intelligence value from the global information infrastructure.<sup>18</sup>

The characteristics of contemporary communications technology mean that the interception of communications by CSE, directed at foreign entities outside Canada, runs the inherent risk of acquiring the private communications of Canadians. It is for this reason that a ministerial authorization is sought for this collection. In addition to the conditions set out in subsection 273.65(2) of the *National Defence Act*, a ministerial directive established other conditions for managing the collection.

My office is undertaking a two-part review of the activities under these ministerial authorizations, as the law is interpreted by the Department of Justice, a point which is discussed below. The objective of this first phase was to provide background to, and criteria for, the detailed review of these complex activities. I provided the Minister of National Defence with a brief report on this study phase in February 2007.

---

<sup>18</sup> “Global information infrastructure” includes electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in, or relating to those emissions, systems or networks. (*National Defence Act*, section 273.61)



---

## Methodology

In order to establish an understanding of this foreign intelligence collection and the unique challenges it presents, this first phase of the review: studied the authorities given to and the conditions imposed upon CSE by the ministerial authorizations, ministerial directive and related articles; and examined how CSE has responded in terms of the policies and procedures that it has developed, and the management framework that has been put in place to oversee these activities.

## Findings

This study phase developed an historical perspective and appreciation of the rationale for this collection activity. It also provided an appreciation of the organizational complexities, the authorities under which it operates, the conditions imposed and the programs in place to implement the authorities while respecting the conditions. Finally, it established the review criteria for the second and final phase, which is now underway.

## Overview of 2006-2007 findings

I am able to report that, overall, the activities of CSE examined during this reporting period complied with the law, with one qualification. It concerned a condition of an information technology security ministerial authorization, which CSE has already undertaken to rectify. A report of CSE's assistance to the RCMP did not provide an assessment of the lawfulness of the activities reviewed, pending a re-examination by CSE of the legal issues raised.

With respect to the review of CSE's signals intelligence collection activities conducted under ministerial authorization, I would highlight once again my disagreement with the Department of Justice's interpretation of the ministerial authorization provisions of the *National Defence Act*. When assessing the lawfulness of activities conducted under ministerial authorizations, I have agreed to use the Department of Justice's interpretation for the present pending amendments to the legislation, which I have already urged be made at the earliest opportunity. I commend the Chief of CSE for supporting this initiative.

## Reviews underway / future reporting

Reviews currently underway that I will be reporting on in the next fiscal year include examinations of CSE's activities related to counter-terrorism, its use of metadata, its support to CSIS, its use of technology to protect the privacy of Canadians, and its activities under a number of foreign intelligence collection and information technology security ministerial authorizations. In addition, my office will begin a number of other reviews, under both my general mandate and my duties under the ministerial authorization provisions.

## Complaints about CSE activities

My mandate includes undertaking any investigation I deem necessary in response to a complaint, to determine whether CSE engaged, or is engaging in unlawful activity.

During the 2006-2007 reporting year my office received no complaints that warranted formal investigation. However, OCSEC did complete one investigation in spring 2006 in response to a complaint that was received in the previous reporting year. A full report was delivered to

the Minister of National Defence outlining the facts of the complaint and the findings resulting from the investigation.

*I am able to report that the investigation found no unlawful activity on the part of CSE.*

While the substance of the complaint is classified, I am able to report that the investigation found no

unlawful activity on the part of CSE. My office made recommendations that were accepted by CSE, and would strengthen compliance.

## Duties under the *Security of Information Act*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy if they wish to claim a "public interest" defence for divulging classified information. No such matters were referred to my office in 2006-2007.

---

## THE COMMISSIONER'S OFFICE

I am supported in my work by a full-time staff of eight. Their extensive experience in the security and intelligence community is supplemented by subject matter experts in areas such as informatics, technology, research, policy development and communications, with whom my office contracts as required.

Many of my office's interests and concerns are shared by other Canadian security and intelligence review agencies. As Justice O'Connor noted, in 2005-2006 my staff initiated the Review Agencies Forum, which brings them together at regular intervals with the staffs of the Security Intelligence Review Committee, the Office of the Inspector General of the Canadian Security Intelligence Service and the Commission for Public Complaints Against the RCMP. In 2006-2007, the Forum met twice to discuss issues such as the recommendations of Justice O'Connor's Policy Review report, and amendments to the *Public Servants Disclosure Act* resulting from the new *Federal Accountability Act* (Bill C-2). In addition, Forum participants discussed how to provide their respective agencies with reasonable turnaround times in responding to reviews, and the different approaches that have been used when delays are encountered.

My staff also participated in other conferences and symposia that provided them with new perspectives on their work, including the International Intelligence Review Agencies Conference in Cape Town, which I described above, and the conferences of the Canadian Association for Security and Intelligence Studies (CASIS) and the Ontario Bar Association. In addition, as a developmental opportunity, my office hosted two promising students at the CASIS conference.

*In 2006-2007, there were some 96,000 visits to my website.*

While my office does not have a formal educational mandate, I do believe it is important that Canadians know about OCSEC's work. To this end, my office hosts a website ([www.csec-ccst.gc.ca](http://www.csec-ccst.gc.ca)) that describes OCSEC's

mandate and activities. Visits to the site originating from outside North America span a global audience ranging from Europe to Asia and the Middle East. In 2006-2007, there were some 96,000 visits to my website.

In 2006-2007, my office's expenditures were \$ 1,267,612, which was well within budget for the period. Annex C to this report provides a summary of 2006-2007 expenditures.

## LOOKING TO THE FUTURE

### The Major Commission of Inquiry and the Iacobucci Internal Inquiry

Two new inquiries that may have an impact on the future review environment are the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, led by the Honourable John Major, and the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, led by the Honourable Frank Iacobucci.

The Air India Commission's mandate is to make findings and recommendations regarding the assessments and actions of Canadian government officials before and after the 1985 bombing, and ways that any past mistakes can be avoided in the future. The Internal Inquiry is mandated to examine all aspects of the involvement of Canadian officials in relation to the detention of the three individuals in Syria or Egypt.

---

## Review methodology

One of the recommendations of the independent operational review of my office conducted in spring 2006 was to document formally the methodology employed by the office to examine CSE's activities. I support this initiative entirely and I am confident that the office will derive benefit from it now and in the longer term. This will be an important preoccupation over the summer months.

## IN CLOSING

Looking back over the last eight months, I would like to express appreciation to my predecessor, the Right Honourable Antonio Lamer, from whom I inherited a fine staff and an organization well positioned to meet the challenges ahead. Thanks to this legacy, I was able to assume my responsibilities immediately upon my appointment, and the transition between our tenures was seamless.

I anticipate continuing the productive relationships that have been established with the Minister of National Defence, with CSE and with officials at other government departments and agencies involved in Canada's security and intelligence community. In particular, I look forward to discussions that I trust will lead to a resolution of the legal interpretation issues that have beset this office since the passage of Part V.1 of the *National Defence Act*.

*I anticipate continuing the productive relationships that have been established.*





## ANNEX A: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

### *National Defence Act – Part V.1*

- 273.63** (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.
- (2) The duties of the Commissioner are
- (a) to review the activities of the Establishment to ensure that they are in compliance with the law;
  - (b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and
  - (c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.
- (3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.
- (4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.
- (5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

- 
- (6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.
- (7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

- 273.65** (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

### *Security of Information Act*

- 15.** (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

- (5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

- (ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

---

## ANNEX B: CLASSIFIED REPORTS, 1996–2007

1. Classified Report to the Minister  
– March 3, 1997 (TOP SECRET)
2. Classified Report to the Minister  
– Operational policies with lawfulness implications – February 6, 1998 (SECRET)
3. Classified Report to the Minister  
– CSE’s activities under \*\*\* – March 5, 1998 (TOP SECRET Codeword/CEO)
4. Classified Report to the Minister  
– Internal investigations and complaints – March 10, 1998 (SECRET)
5. Classified Report to the Minister  
– CSE’s activities under \*\*\* – December 10, 1998 (TOP SECRET/CEO)
6. Classified Report to the Minister  
– On controlling communications security (COMSEC) material – May 6, 1999  
(TOP SECRET)
7. Classified Report to the Minister  
– How we test (A classified report on the testing of CSE’s signals intelligence collection and holding practices, and an assessment of the organization’s efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)
8. Classified Report to the Minister  
– A study of the \*\*\* collection program – November 19, 1999 (TOP SECRET Codeword/CEO)
9. Classified Report to the Minister  
– On \*\*\* – December 8, 1999 (TOP SECRET/COMINT)
10. Classified Report to the Minister  
– A study of CSE’s \*\*\* reporting process — an overview (Phase I)  
– December 8, 1999 (SECRET/CEO)
11. Classified Report to the Minister  
– A study of selection and \*\*\* — an overview – May 10, 2000 (TOP SECRET/CEO)

12. Classified Report to the Minister
  - CSE’s operational support activities under \*\*\* — follow-up – May 10, 2000 (TOP SECRET/CEO)
13. Classified Report to the Minister
  - Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)
14. Classified Report to the Minister
  - On findings of an external review of CSE’s ITS program – June 15, 2000 (SECRET)
15. Classified Report to the Minister
  - CSE’s policy system review – September 13, 2000 (TOP SECRET/CEO)
16. Classified Report to the Minister
  - A study of the \*\*\* reporting process — \*\*\* (Phase II) – April 6, 2001 (SECRET/CEO)
17. Classified Report to the Minister
  - A study of the \*\*\* reporting process — \*\*\* (Phase III) – April 6, 2001 (SECRET/CEO)
18. Classified Report to the Minister
  - CSE’s participation \*\*\* – August 20, 2001 (TOP SECRET/CEO)
19. Classified Report to the Minister
  - CSE’s support to \*\*\*, as authorized by \*\*\* and code-named \*\*\*  
– August 20, 2001 (TOP SECRET/CEO)
20. Classified Report to the Minister
  - A study of the formal agreements in place between CSE and various external parties in respect of CSE’s Information Technology Security (ITS)  
– August 21, 2002 (SECRET)
21. Classified Report to the Minister
  - CSE’s support to \*\*\*, as authorized by \*\*\* and code-named \*\*\*  
– November 13, 2002 (TOP SECRET/CEO)



- 
22. Classified Report to the Minister
    - CSE’s \*\*\* activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)
  23. Classified Report to the Minister
    - Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)
  24. Classified Report to the Minister
    - CSE’s activities pursuant to \*\*\* Ministerial authorizations including \*\*\*
      - May 20, 2003 (SECRET)
  25. Classified Report to the Minister
    - CSE’s support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part I
      - November 6, 2003 (TOP SECRET/COMINT/CEO)
  26. Classified Report to the Minister
    - CSE’s support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part II
      - March 15, 2004 (TOP SECRET/COMINT/CEO)
  27. Classified Report to the Minister
    - A review of CSE’s activities conducted under \*\*\* Ministerial authorization
      - March 19, 2004 (SECRET/CEO)
  28. Classified Report to the Minister
    - Internal investigations and complaints — follow-up – March 25, 2004 (TOP SECRET/CEO)
  29. Classified Report to the Minister
    - A review of CSE’s activities conducted under 2002 \*\*\* Ministerial authorization
      - April 19, 2004 (SECRET/CEO)
  30. Classified Report to the Minister
    - Review of CSE \*\*\* operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)
  31. Classified Report to the Minister
    - CSE’s support to \*\*\* – January 7, 2005 (TOP SECRET/COMINT/CEO)

32. Classified Report to the Minister
  - External review of CSE's \*\*\* activities conducted under Ministerial authorization
  - February 28, 2005 (TOP SECRET/COMINT/CEO)
33. Classified Report to the Minister
  - A study of the \*\*\* collection program – March 15, 2005 (TOP SECRET/COMINT/CEO)
34. Classified Report to the Minister
  - Report on the activities of CSE's \*\*\* – June 22, 2005 (TOP SECRET)
35. Classified Report to the Minister
  - Interim report on CSE's \*\*\* operations conducted under Ministerial authorization
  - March 2, 2006 (TOP SECRET/COMINT)
36. Classified Report to the Minister
  - External review of CSE \*\*\* activities conducted under Ministerial authorization
  - March 29, 2006 (TOP SECRET/CEO)
37. Classified Report to the Minister
  - Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – June 16, 2006 (TOP SECRET/COMINT/CEO)
38. Classified Report to the Minister
  - Review of information technology security activities at a government department under ministerial authorization – December 18, 2006 (TOP SECRET)
39. Classified Report to the Minister
  - Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – February 20, 2007 (TOP SECRET/COMINT/CEO)
40. Classified Report to the Minister
  - Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – March 31, 2007 (TOP SECRET/COMINT/CEO)

---

## ANNEX C: STATEMENT OF EXPENDITURES 2006–2007

### Standard Object Summary

Salaries and Wages	\$594,551
Transportation and Telecommunications	72,839
Information	14,071
Professional and Special Services	402,620
Rentals	140,315
Purchased Repair and Maintenance	4,649
Materials and Supplies	6,404
Acquisition of Machinery and Equipment	29,977
Other Expenditures	2,186
<b>Total</b>	<b>\$1,267,612</b>



---

## ANNEX D: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

The Office of the Communications Security Establishment Commissioner (OCSEC) was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Quebec, who held the position until June 2003. He was succeeded by the Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., Chief Justice of Canada (retired) for a term of three years. The Honourable Charles D. Gonthier, Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act*. During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment (CSE) to determine whether they conformed with the laws of Canada; and to receive complaints about CSE's activities.

Following the terrorist attacks in the United States on September 11, 2001, Parliament adopted the omnibus *Anti-Terrorism Act* which came into force on December 24, 2001. The omnibus *Act* introduced amendments to the *National Defence Act*, by adding Part V.1 and creating legislative frameworks for both OCSEC and CSE. It also gave the Commissioner new responsibilities to review activities carried out by CSE under a ministerial authorization.

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act*. This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSE on the grounds that it is in the public interest.

Under the Commissioner's current mandate, which entrenched in law the original mandate established in 1996 as well as the additional responsibilities described above, the Commissioner has retained the powers of a commissioner under Part II of the *Inquiries Act*.





---

## ANNEX E: ROLE AND MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT

The Communications Security Establishment (CSE) is Canada's national cryptologic agency. Unique within Canada's security and intelligence community, CSE employs code-makers and code-breakers to provide the Government of Canada with information technology security and foreign signals intelligence services. CSE also provides technical and operational assistance to federal law enforcement and security agencies.

CSE's foreign signals intelligence products and services support government decision-making in the fields of national security, national intelligence and foreign policy. CSE's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSE's information technology security products and services enable its clients (other government departments and agencies) to effectively secure their electronic information systems and networks. CSE also conducts research and development on behalf of the Government of Canada in fields related to communications security.

CSE has a three-part mandate under Part V.1, subsection 273.64(1) of the *National Defence Act*. These are known as the (a) (b) and (c) mandates:

- (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
- (b) to provide advice, guidance and services to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada; and
- (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.





Le Centre de la sécurité des télécommunications (CST) est l'organisme national de cryptologie du Canada. Organisme unique en son genre de la collectivité canadienne de la sécurité et du renseignement, le CST emploie des cryptologues pour protéger la sécurité des technologies de l'information du gouvernement du Canada et lui fournir des renseignements électromagnétiques étrangers. Il offre en outre une assistance technique et opérationnelle aux organismes fédéraux chargés de la sécurité et de l'application de la loi.

Les produits et services de renseignement électromagnétique étranger du CST sont fournis à l'appui des décisions gouvernementales dans les domaines de la sécurité nationale, du renseignement national et de la politique étrangère. Ses activités en la matière visent exclusivement des renseignements étrangers et sont assujetties aux priorités du gouvernement du Canada en matière de renseignement.

Dans le domaine de la sécurité des technologies de l'information, les produits et services du CST permettent à ses clients (les autres ministères et organismes gouvernementaux) d'assurer la sécurité de leurs systèmes et réseaux d'information électronique. Le CST effectue aussi des travaux de recherche-développement au nom du gouvernement du Canada dans des disciplines liées à la sécurité des télécommunications.

Le paragraphe 273.64(1) de la partie V.1 de la *Loi sur la défense nationale* établit le mandat du CST, qui comprend trois volets désignés sous le nom de parties a), b) et c) :

- a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
- b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;
- c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.





## ANNEXE D : HISTORIQUE DU BUREAU DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) a été créé le 19 juin 1996, au moment de la nomination du premier commissaire, l'honorable Claude Bissson, O.C., ancien juge en chef du Québec. M. Bissson a occupé le poste de commissaire jusqu'en juin 2003. Le très honorable Antonio Lamer, c.p., C.C., c.d., LL.D., d.n., juge en chef du Canada (à la retraite), lui a alors succédé pour un mandat de trois ans. L'honorable Charles D. Gonthier, c.r., qui a pris sa retraite de la Cour suprême du Canada en 2003, a été nommé commissaire en août 2006.

Pendant les six premières années de son mandat (de juin 1996 à décembre 2001), le commissaire a exercé ses fonctions conformément à plusieurs décrets, pris en vertu de la partie II de la *Loi sur les enquêtes*. Au cours de cette période, il a assumé une double responsabilité : examiner les activités du Centre de la sécurité des télécommunications (CST) afin de déterminer si elles étaient en conformité avec les lois du Canada, et recevoir les plaintes relatives aux activités du CST.

Dans le sillage des attentats terroristes du 11 septembre 2001, le Parlement a adopté la *Loi antiterroriste omnibus*, qui a été promulguée le 24 décembre 2001. Cette loi modifie la *Loi sur la défense nationale*, en y ajoutant la partie V.1, qui établit le cadre législatif du BCCST et du CST, et elle confie au commissaire de nouvelles responsabilités relatives à l'examen des activités que mène le CST sous le régime d'une autorisation ministérielle.

En outre, la *Loi omnibus* a remplacé la *Loi sur les secrets officiels* par la *Loi sur la protection de l'information*, laquelle attribue au commissaire des fonctions précises pour les cas où une personne astreinte au secret à perpétuité souhaiterait invoquer la défense de l'intérêt public pour justifier la divulgation de renseignements classifiés sur le CST.

En vertu de son mandat actuel, qui inscrit dans la loi le mandat initial établi en 1996 ainsi que les nouvelles responsabilités supplémentaires décrites ci-dessus, le commissaire conserve tous les pouvoirs que confère à un commissaire la partie II de la *Loi sur les enquêtes*.



## ANNEXE C : ÉTAT DES DÉPENSES, 2006-2007

### Sommaire des articles courants

Traitements et salaires	594 551 \$
Transports et télécommunications	72 839
Information	14 071
Services professionnels et spéciaux	402 620
Location	140 315
Achat de services de réparation et d'entretien	4 649
Fournitures et approvisionnements	6 404
Acquisition de machine et de matériel	29 977
Autres charges	2 186
Total	1 267 612 \$

32. Classified Report to the Minister  
– External review of CSE's \*\*\* activities conducted under Ministerial authorization – 28 février 2005 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
33. Classified Report to the Minister  
– A study of the \*\*\* collection program – 15 mars 2005 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
34. Classified Report to the Minister  
– Report on the activities of CSE's \*\*\* – 22 juin 2005 (TRÈS SECRET)
35. Classified Report to the Minister  
– Interim report on CSE's \*\*\* operations conducted under Ministerial authorization – 2 mars 2006 (TRÈS SECRET/COMINT)
36. Classified Report to the Minister  
– External review of CSE's \*\*\* activities conducted under Ministerial authorization – 29 mars 2006 (TRÈS SECRET/Réserve aux Canadiens)
37. Classified Report to the Minister  
– Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – 16 juin 2006 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
38. Classified Report to the Minister  
– Review of information technology security activities at a government department under ministerial authorization – 18 décembre 2006 (TRÈS SECRET)
39. Classified Report to the Minister  
– Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – 20 février 2007 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
40. Classified Report to the Minister  
– Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – 31 mars 2007 (TRÈS SECRET/COMINT/Réserve aux Canadiens)



22. Classified Report to the Minister  
– CSE's \*\*\* activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization  
– 27 novembre 2002 (TRÈS SECRET/Réserve aux Canadiens)
23. Classified Report to the Minister  
– Lexicon of CSE definitions – 26 mars 2003 (TRÈS SECRET)
24. Classified Report to the Minister  
– CSE's activities pursuant to \*\*\* Ministerial authorizations including \*\*\*  
– 20 mai 2003 (SECRET)
25. Classified Report to the Minister  
– CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part I  
– 6 novembre 2003 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
26. Classified Report to the Minister  
– CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part II  
– 15 mars 2004 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
27. Classified Report to the Minister  
– A review of CSE's activities conducted under \*\*\* Ministerial authorization  
– 19 mars 2004 (SECRET/Réserve aux Canadiens)
28. Classified Report to the Minister  
– Internal investigations and complaints — follow-up – 25 mars 2004  
(TRÈS SECRET/Réserve aux Canadiens)
29. Classified Report to the Minister  
– A review of CSE's activities conducted under 2002 \*\*\* Ministerial authorization  
– 19 avril 2004 (SECRET/Réserve aux Canadiens)
30. Classified Report to the Minister  
– Review of CSE \*\*\* operations under Ministerial authorization – 1<sup>er</sup> juin 2004  
(TRÈS SECRET/COMINT)
31. Classified Report to the Minister  
– CSE's support to \*\*\* – 7 janvier 2005 (TRÈS SECRET/COMINT/  
Réserve aux Canadiens)

11. Classified Report to the Minister  
 – A study of selection and \*\*\* — an overview — 10 mai 2000 (TRÈS SECRET/Réserve aux Canadiens)
12. Classified Report to the Minister  
 – CSE's operational support activities under \*\*\* — follow-up — 10 mai 2000 (TRÈS SECRET/Réserve aux Canadiens)
13. Classified Report to the Minister  
 – Internal investigations and complaints — follow-up — 10 mai 2000 (SECRET)
14. Classified Report to the Minister  
 – On findings of an external review of CSE's ITS program — 15 juin 2000 (SECRET)
15. Classified Report to the Minister  
 – CSE's policy system review — 13 septembre 2000 (TRÈS SECRET/Réserve aux Canadiens)
16. Classified Report to the Minister  
 – A study of the \*\*\* reporting process — \*\*\* (Phase II) — 6 avril 2001 (SECRET/Réserve aux Canadiens)
17. Classified Report to the Minister  
 – A study of the \*\*\* reporting process — \*\*\* (Phase III) — 6 avril 2001 (SECRET/Réserve aux Canadiens)
18. Classified Report to the Minister  
 – CSE's participation \*\*\* — 20 août 2001 (TRÈS SECRET/Réserve aux Canadiens)
19. Classified Report to the Minister  
 – CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — 20 août 2001 (TRÈS SECRET/Réserve aux Canadiens)
20. Classified Report to the Minister  
 – A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) — 21 août 2002 (SECRET)
21. Classified Report to the Minister  
 – CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — 13 novembre 2002 (TRÈS SECRET/Réserve aux Canadiens)

1. Classified Report to the Minister  
– 3 mars 1997 (TRÈS SECRET)
2. Classified Report to the Minister  
– Operational policies with lawfulness implications – 6 février 1998 (SECRET)
3. Classified Report to the Minister  
– CSE's activities under \*\*\* – 5 mars 1998 (TRÈS SECRET Mot codé/  
Réservé aux Canadiens)
4. Classified Report to the Minister  
– Internal investigations and complaints – 10 mars 1998 (SECRET)
5. Classified Report to the Minister  
– CSE's activities under \*\*\* – 10 décembre 1998 (TRÈS SECRET/Réservé aux  
Canadiens)
6. Classified Report to the Minister  
– On controlling communications security (COMSEC) material – 6 mai 1999  
(TRÈS SECRET)
7. Classified Report to the Minister  
– How we test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière  
de collecte et de conservation de renseignements électromagnétiques, et évaluation  
des efforts de l'organisme pour sauvegarder la vie privée des Canadiens)  
– 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)
8. Classified Report to the Minister  
– A study of the \*\*\* collection program – 19 novembre 1999 (TRÈS SECRET  
Mot codé/Réservé aux Canadiens)
9. Classified Report to the Minister  
– On \*\*\* – 8 décembre 1999 (TRÈS SECRET/COMINT)
10. Classified Report to the Minister  
– A study of CSE's \*\*\* reporting process — an overview (Phase I)  
– 8 décembre 1999 (SECRET/Réservé aux Canadiens)

- (7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.
- [...]
- 273.65** (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.
- Loi sur la protection de l'information*
15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]
- (5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]
- b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession : [...]
- (ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.

273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

- a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;
- b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;
- c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la Loi sur les enquêtes.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.





L'une des recommandations issues de l'examen opérationnel indépendant des activités de mon bureau réalisé au printemps 2006 préconisait de documenter officiellement la méthodologie utilisée par le Bureau pour examiner les activités du CST. J'appuie sans réserve cette recommandation et je suis convaincu que le Bureau en bénéficiera tant dans l'immédiat qu'à long terme. Ce sera là une de ses préoccupations importantes au cours de l'été.

## Conclusion

Au moment de prendre acte du bilan des huit derniers mois, j'aimerais exprimer ma gratitude à mon prédécesseur, le très honorable Antonio Lamer, de qui j'ai hérité d'un excellent personnel et d'une organisation bien placée pour relever les défis qui l'attendent. Grâce à cet héritage, j'ai été en mesure de m'acquitter de mes responsabilités au moment même de ma nomination, et la transition s'est fait sans heurt.

Je compte entretenir les rapports productifs qui ont été mis en place avec le ministre de la Défense nationale, le CST et les représentants des autres ministères et organismes du gouvernement qui font partie de la collectivité canadienne du renseignement et de la sécurité. J'attends avec impatience en particulier la tenue de discussions qui nous permettront, je l'espère, de régler les questions d'interprétation de la loi avec lesquelles le BCCST est aux prises depuis l'adoption de la partie V.1 de la *Loi sur la défense nationale*.

été mis en place.

Je compte entretenir les

rapports productifs qui ont

été mis en place.

En 2006-2007, mon site Web a reçu quelque 96 000 visites.

Bien que mon bureau n'ait pas de mandat éducatif officiel, je crois qu'il est important que les Canadiens sachent ce que fait le BCCST. Le Bureau possède donc un site Web ([www.csec-ccst.gc.ca](http://www.csec-ccst.gc.ca)), qui décrit son mandat et ses activités. Le site attire un public international au-delà du continent nord américain, notamment des visiteurs d'Europe, d'Asie et du Moyen-Orient. En 2006-2007, mon site Web a reçu quelque 96 000 visites.

En 2006-2007, les dépenses de mon bureau se sont chiffrées à 1 267 612 \$, et ont été largement couvertes par le budget approuvé pour cette période. On trouvera un résumé de ces dépenses à l'annexe C.

## REGARD SUR L'AVENIR

### Commission d'enquête Major et Enquête interne Iacobucci

Deux nouvelles enquêtes pourraient avoir des répercussions sur le contexte des futurs examens : la Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat à la bombe commis contre le vol 182 d'Air India, présidée par l'honorable John Major, et l'Enquête interne sur les actions des responsables canadiens relativement à Abdullah Almaliki, Ahmad Abou-Elmaati et Muayyed Nureddin, présidée par l'honorable Frank Iacobucci.

La Commission sur l'affaire d'Air India a pour mandat de faire part au gouvernement de ses conclusions et recommandations sur les analyses et les actions des représentants du gouvernement canadien avant et après les attentats à la bombe de 1985, ainsi que sur les mesures à prendre pour éviter que toute erreur ne se reproduise. L'Enquête interne a pour mandat d'examiner tous les aspects de la participation des responsables canadiens relativement à la détention des trois personnes concernées en Syrie ou en Egypte.

Pour accomplir mon mandat, je suis secondé par un effectif de huit employés à temps plein qui possèdent une vaste expérience au sein de la collectivité de la sécurité et du renseignement. Nous avons en outre parfois recours à des spécialistes de divers domaines, notamment l'informatique, les technologies, la recherche, l'élaboration des politiques et les communications, que nous embauchons à contrat selon les besoins.

Mon bureau partage souvent les mêmes intérêts et préoccupations que d'autres organismes canadiens de surveillance de la sécurité et du renseignement. Comme l'a mentionné le juge O'Connor, les employés de mon bureau ont mis sur pied en 2005-2006 la Tribune des organismes d'examen, qui leur permet de rencontrer à intervalle régulier les employés du Comité de surveillance des activités de renseignement de sécurité, du Bureau de l'Inspecteur général du Service canadien du renseignement de sécurité et de la Commission des plaintes du public contre la GRC. En 2006-2007, les membres de la Tribune se sont réunis à deux reprises pour discuter de diverses questions, notamment des recommandations contenues dans le rapport sur l'examen de la politique du juge O'Connor, ainsi que des modifications à la *Loi sur la protection des fonctionnaires divulgués d'actes répréhensibles* résultant de la nouvelle *Loi fédérale sur la responsabilité* (projet de loi C-2). Les membres de la Tribune ont, en outre, discuté des façons de fournir à leurs organismes respectifs des délais raisonnables pour répondre aux examens, ainsi que des différentes manières de procéder lorsque des retards se produisent.

Les employés de mon bureau ont, de plus, participé à d'autres conférences et symposiums, notamment la conférence internationale des organes de surveillance du renseignement qui a eu lieu au Cap, dont j'ai parlé précédemment, et aux conférences de l'Association canadienne pour les études de renseignement et de sécurité (ACERS) et de l'Association du Barreau de l'Ontario. De plus, mon bureau a accueilli deux étudiants prometteurs à la conférence de l'ACERS pour leur offrir une occasion de perfectionnement.

## Examens en cours / rapports à venir

Au cours du prochain exercice financier, je ferai rapport sur divers examens actuellement en cours qui portent notamment sur les activités du CST liées à l'antiterrorisme, son utilisation des métadonnées, son soutien au SCRS, à l'utilisation des technologies pour protéger la vie privée des Canadiens et ses activités touchant la collecte de renseignements étrangers et la protection de la sécurité des technologies de l'information menées sous le régime de plusieurs autorisations ministérielles. De plus, mon bureau entreprendra divers autres examens, qui seront réalisés dans le cadre de mon mandat général ou de mes fonctions découlant des dispositions sur les autorisations ministérielles.

## Plaintes relatives aux activités du CST

Dans le cadre de mon mandat, je dois procéder à toute enquête que je considère nécessaire par suite d'une plainte, afin de déterminer si certaines activités du CST ont été ou sont illégales.

Au cours de l'année 2006-2007, mon bureau n'a reçu aucune plainte ayant nécessité une enquête officielle. Au printemps 2006, il a toutefois terminé une enquête relative à une plainte reçue l'année précédente. Un rapport complet détaillant les faits et les conclusions de l'enquête a été remis au

ministre de la Défense nationale.

Bien que les renseignements sur cette plainte soient classifiés, je suis en mesure de rapporter

que l'enquête n'a révélé aucune activité illégale de la part du CST. Mon bureau a présenté au

CST des recommandations qui ont été acceptées et qui permettront de renforcer la conformité.

## Fonctions exercées en vertu de la Loi sur la protection de l'information

La Loi sur la protection de l'information m'autorise à recevoir des renseignements de personnes astreintes au secret à perpétuité qui veulent se prévaloir de la défense « d'intérêt public » concernant la divulgation de renseignements classifiés. Aucun problème de ce genre n'a été soumis à mon bureau en 2006-2007.

*Je suis en mesure de*

*rapporter que l'enquête n'a*

*révélé aucune activité*

*illégale de la part du CST.*



Afin de bien comprendre cette forme de collecte de renseignements étrangers et les défis particuliers qu'elle présente, la première partie de l'examen comportait : l'examen des pouvoirs conférés et des conditions imposées au CST par les autorisations ministérielles, la directive ministérielle et les dispositions connexes; l'examen des politiques et des procédures que le CST a élaborées en la matière, ainsi que du cadre de gestion qu'il a mis en place pour superviser ces activités.

## Conclusions

Cette partie de l'examen nous a permis de comprendre l'historique de cette activité et sa raison d'être. Elle nous a également permis de mieux comprendre les complexités organisationnelles qui l'entourent, les autorisations qui la régissent, ainsi que les conditions imposées et les programmes en place pour mettre en œuvre les autorisations, tout en respectant les conditions qui y sont attachées. Enfin, cette partie nous a en outre permis d'établir les critères régissant la deuxième et dernière partie de l'examen, qui est en cours actuellement.

## Aperçu des conclusions pour 2006-2007

Je suis à même de déclarer que, dans l'ensemble, les activités du CST examinées pendant la période de référence sont conformes à la loi, sauf dans un cas. Ce cas concerne l'une des conditions d'une autorisation ministérielle visant à vérifier la sécurité des technologies de l'information. Le CST a déjà entrepris de corriger la situation. Un rapport sur l'assistance fournie à la GRC ne contenait pas d'évaluation de la légalité des activités à l'examen, le CST devant réexaminer les questions juridiques soulevées.

Pour ce qui est des activités de collecte de renseignements électromagnétiques effectuées par le CST sous le régime d'une autorisation ministérielle, je tiens à réitérer mon désaccord sur l'interprétation donnée par le ministère de la Justice aux dispositions de la *Loi sur la défense nationale* à cet égard. J'ai accepté d'évaluer la légalité des activités du CST menées en vertu de ces autorisations en me fondant sur cette dernière interprétation en attendant que la loi soit modifiée à la première occasion comme j'en ai signalé l'urgence. Je sais gré au chef du CST de son appui à ces modifications.

étaient, entre autres, de fournir une formation plus complète aux clients qui présentent des demandes et d'accorder à plus de clients un accès électronique sécurisé afin de réduire les risques d'erreur et d'améliorer le contrôle du processus. Je suis heureux de constater que depuis l'examen, le CST a en outre accru la formation et la supervision de son personnel qui travaille dans la Section des politiques opérationnelles en ce qui a trait à la divulgation des renseignements supprimés.

## Examen des activités de collecte de renseignements électromagnétiques menées par le CST sous le régime d'une autorisation ministérielle

### Contexte

Des activités de collecte de renseignements étrangers ont été menées sous le régime de trois autorisations ministérielles qui ont été en vigueur de mars 2004 à décembre 2006. Ces autorisations ministérielles visaient l'interception de communications utiles aux fins du renseignement étranger, sur l'infrastructure mondiale d'information<sup>18</sup>.

Compte tenu des caractéristiques des technologies de communication modernes, le CST court le risque inhérent, lorsqu'il tente d'intercepter les communications d'entités qui se trouvent à l'étranger, d'intercepter en même temps des communications privées de Canadiens. C'est pourquoi il doit obtenir une autorisation ministérielle à cette fin. En plus des conditions prévues au paragraphe 273.65(2) de la *Loi sur la défense nationale*, la directive ministérielle stipule d'autres conditions régissant la gestion des renseignements recueillis.

Mon bureau procède à un examen en deux parties des activités menées sous le régime de ces autorisations ministérielles, suivant l'interprétation donnée de la loi par le ministère de la Justice, qui est discutée ci-après. L'objectif de la première partie était d'établir un contexte et des critères pour pouvoir procéder à un examen en profondeur de ces activités complexes. J'ai remis au ministre de la Défense nationale un rapport sommaire sur cette partie de l'examen en février 2007.

<sup>18</sup> « Infrastructure mondiale d'information » s'entend notamment des émissions électromagnétiques, des systèmes de communication, des systèmes et réseaux des techniques de l'information ainsi que des données et des renseignements techniques qu'ils transportent, qui s'y trouvent ou qui les concernent. (*Loi sur la défense nationale*, article 273.61)

rapports sur le renseignement, expliquent aux clients individuels et potentiels le rôle du CST et du renseignement électromagnétique, et aident à établir les besoins des clients en fonction des priorités du gouvernement du Canada en matière de renseignement.

Pour protéger la vie privée, le CST supprime dans ses rapports sur le renseignement étranger les données personnelles qui concernent des Canadiens. Si un client a l'autorisation nécessaire et le besoin de connaître cette information, il peut l'obtenir en présentant une demande officielle accompagnée de preuves justificatives. Toutes les demandes de divulgation de renseignements sont acheminées à la Section des politiques opérationnelles du CST.

La majorité des demandes est maintenant acheminée directement au CST par l'entremise d'un réseau de communication sécurisé. Les agents des relations avec la clientèle jouent un rôle dans la divulgation de ces renseignements parce qu'ils traitent les demandes des clients qui n'ont pas accès à ce réseau sécurisé.

## Méthodologie

L'examen a consisté à examiner les documents pertinents, notamment les pouvoirs qui régissent les activités des agents des relations avec la clientèle et l'unité du CST autorisée à divulguer l'information. Toutes les demandes de divulgation et les divulgations comme telles de renseignements supprimés sur une période de six mois ont été passées au peigne fin pour vérifier leur conformité avec la loi et la politique. Des entrevues ont été menées avec les agents des relations avec la clientèle, leurs gestionnaires, ainsi qu'avec le gestionnaire de la Section des politiques opérationnelles.

## Conclusions

L'examen a permis de conclure que les activités des agents des relations avec la clientèle et de la Section des politiques opérationnelles du CST étaient conformes à la *Loi sur la défense nationale* et aux politiques connexes du CST. Nous avons constaté toutefois quelques incohérences dans les demandes et les divulgations. Nous avons en outre constaté que la politique et la pratique pourraient être améliorées à certains égards afin de mieux protéger les renseignements personnels, comme l'exige la *Loi sur la protection des renseignements personnels*. Les recommandations à ce sujet

L'objectif de cet examen était d'évaluer la légalité des activités à la fois des agents des relations avec la clientèle et de la Section des politiques opérationnelles du CST en ce qui a trait à la demande et à la divulgation de renseignements personnels sur des Canadiens, qui ont été supprimés des rapports du CST sur le renseignement étranger (dont nous avons parlé précédemment). L'information est mise à la disposition des clients autorisés du gouvernement du Canada à certaines conditions seulement.

Depuis sa création en 1946, le CST fournit des rapports sur le renseignement étranger basés sur des renseignements d'origine électromagnétique aux responsables concernés des ministères. Ces rapports étaient remis en main propre jusqu'à la création en 1985 du programme des agents des relations avec la clientèle sur place. Ces agents fournissent des

## Contexte

# Examen des rôles des agents des relations avec la clientèle et de la Section des politiques opérationnelles du CST dans la divulgation de renseignements personnels

L'examen a révélé que le processus d'acquisition par le CST de l'autorisation ministérielle nécessaire pour mener ses activités au sein du ministère était conforme aux exigences de la *Loi sur la défense nationale*. L'examen a en outre révélé que quatre des cinq conditions prévues au paragraphe 273.65(4) de la *Loi* étaient remplies. En ce qui concerne l'une d'entre elles toutefois, l'examen a fait ressortir que certains renseignements ont été conservés, même si leur conservation n'était pas essentielle. Bien que le personnel du CST ait agi conformément aux directives reçues, certains éléments pourraient être améliorés, et le CST a entrepris de le faire. Le CST a en outre indiqué que les prochains protocoles d'entente qui seront conclus avec ses ministères clients concernant des activités liées à la protection de la sécurité des technologies de l'information qui sont menées sous le régime d'une autorisation ministérielle rendront compte de ces améliorations.

Les autres recommandations issues de l'examen sont, entre autres, de veiller à ce que les pratiques et politiques du CST touchant les tâches confiées à son personnel au cours des activités menées dans le but de protéger la sécurité des technologies de l'information favorisent la conformité avec les pouvoirs que la loi confère au CST.



Les personnes qui communiquent avec le gouvernement pour des raisons

personnelles ou d'affaires ont des attentes

raisonnables touchant la protection de leur vie

privée. Toutefois, en effectuant des tests pour

vérifier si les réseaux et les systèmes

d'informationnel du gouvernement sont bien

protégés, il arrive parfois que des communications

privées ou des renseignements personnels soient

interceptés par inadvertance. Le paragraphe

273.65(3) de la *Loi sur la défense nationale* prévoit

ce qui suit :

Les personnes qui

communiquent avec le

gouvernement pour des

raisons personnelles ou

d'affaires ont des attentes

raisonnables touchant la

protection de leur vie privée.

Le ministre peut, dans le seul but de protéger les systèmes ou les

réseaux informatiques du gouvernement du Canada de tout méfait

ou de toute utilisation non autorisée ou de toute perturbation de

leur fonctionnement, autoriser par écrit le Centre de la sécurité des

télécommunications à intercepter, dans les cas visés à l'alinéa

184(2)c) du *Code criminel*, des communications privées qui sont

liées à une activité ou une catégorie d'activités qu'il mentionne

expressément.

Dans ce cas, le CST a la responsabilité de demander une autorisation au

nom du ministre ou de l'organisme pour demander que l'activité soit

couverte. L'autorisation ministérielle permet au CST de procéder à une

évaluation complète des réseaux et systèmes informatiques d'un ministre.

## Méthodologie

L'examen a consisté dans un premier temps à examiner les documents et

dossiers liés à l'autorisation ministérielle et les conditions imposées par

cette dernière. On a ensuite procédé à des entrevues d'enquête et de

vérification avec le CST et les représentants de certains clients qui avaient

participé directement au processus d'autorisation ou aux activités qui ont

sui.

## Conclusions

Sous la réserve ci-dessous au sujet d'une des conditions prévues dans

l'autorisation ministérielle, l'examen a révélé que les activités du CST

effectuées au sein du ministère étaient conformes à la loi et respectaient les

dispositions de l'autorisation ministérielle.



c'est-à-dire remplacées par une référence générique telle que « un Canadien ». Par la suite, quand il reçoit une demande de divulgation de renseignements personnels sur des Canadiens, le CST exige de son client, y compris la GRC, qu'il justifie son droit d'obtenir cette information en vertu de son propre mandat et qu'il fournisse une justification opérationnelle de son besoin de connaître ces renseignements. Si ces conditions sont réunies, le CST divulgue l'information.

Un examen approfondi des articles pertinents de la *Loi sur la défense nationale* et de la *Loi sur la protection des renseignements personnels* a soulevé la question du respect, par le CST, des diverses autorisations régissant la divulgation. C'est pourquoi mon bureau a recommandé que le CST réexamine aussi ses pouvoirs en matière de collecte, d'utilisation et de divulgation de renseignements personnels à certains ministères et organismes fédéraux. De plus, il a recommandé que le CST conclue des ententes avec ses clients, afin d'officialiser les situations dans lesquelles il peut divulguer ces renseignements lorsqu'il fournit une assistance en vertu de la partie c) de son mandat.

Le CST a reconnu que le rapport soulevait diverses questions qui, d'un point de vue stratégique/juridique, nécessiteront une analyse approfondie de la part du CST et du conseiller juridique du ministère de la Justice. Je prévois que cette analyse comprendra une étude et peut-être une prise de position officielle et claire de la part du CST sur l'application de la *Loi sur la défense nationale* en ce qui a trait à la prestation de renseignements étrangers en conformité avec les priorités du gouvernement du Canada en matière de renseignement.

## Examen des activités liées à la protection de la sécurité des technologies de l'information au sein d'un ministère

### Contexte

L'examen a porté sur les activités liées à la protection de la sécurité des technologies de l'information exercées par le CST sous le régime d'une autorisation ministérielle en 2004-2005 au sein d'un ministère. L'objectif était d'évaluer et de vérifier si ces activités étaient conformes à la loi et respectaient les dispositions de l'autorisation ministérielle.

Nombre de conclusions et recommandations contenues dans le premier rapport de mon bureau s'appliquent également à la deuxième phase de l'examen des activités d'assistance fournies en vertu de la partie a) du mandat du CST, notamment la recommandation qui lui a été faite de modifier ou de mettre à jour les instruments sur lesquels s'appuie le soutien qu'il offre à la GRC. Mon prédécesseur était heureux d'annoncer que le CST avait accepté la plupart de ces recommandations et qu'il s'employait à les mettre en œuvre.

Le CST a indiqué qu'il accordait une très haute importance à l'élaboration et à la mise en place d'un système de gestion des dossiers.

Le CST a, par ailleurs, reconnu la nécessité de mettre en place un système officiel de tenue des dossiers. Cet aspect demeure une source de préoccupation, comme le mentionne le Rapport annuel 2005-2006 de mon bureau. Le CST a indiqué qu'il accordait une très haute importance à l'élaboration et à la mise en place d'un système de gestion des dossiers électroniques et imprimés répondant à ses besoins.

Pendant la deuxième phase de l'examen, une vérification approfondie de la réponse du CST aux demandes de renseignements de la GRC a fait ressortir deux sources de préoccupation exigeant un examen juridique plus approfondi de la part du CST. La première était de savoir si les demandes de renseignements de la GRC dans le cadre de ses enquêtes criminelles au pays relèvent de la partie a) du mandat du CST. En attendant que le CST réexamine la question, la légalité de ses activités d'assistance à cet organisme en vertu de la partie a) de son mandat tel qu'il est actuellement interprété et appliqué par le CST n'a pas été évaluée. Le personnel de mon bureau suit le dossier.

La deuxième source de préoccupation concernait les politiques et pratiques du CST en matière de divulgation de renseignements personnels sur des Canadiens à ses clients. Lorsqu'il recueille des renseignements étrangers, le CST peut incidemment acquérir des renseignements personnels sur des Canadiens. Il peut conserver ces renseignements s'il les juge indispensables à la compréhension des renseignements étrangers et les inclure dans ses rapports sur le renseignement étranger pour autant qu'ils soient supprimés,

## POINTS SAILLANTS EN 2006-2007

### Examen des activités de collecte de renseignements étrangers effectuées par le CST à l'appui des activités de la GRC

#### Contexte

En janvier 2005, mon bureau a présenté un rapport au ministre de la Défense nationale sur les résultats de son examen des activités d'assistance technique et opérationnelle fournies par le CST à la GRC en vertu de l'alinéa 273.64(1)c) de la *Loi sur la défense nationale*, communément appelé partie c) du mandat du CST<sup>17</sup>. Après la deuxième et dernière phase de l'examen, mon prédécesseur a présenté, en juin 2006, un rapport de suivi sur l'examen des activités de collecte de renseignements électromagnétiques étrangers effectuées par le CST à l'appui de la GRC, en vertu de l'alinéa 273.64(1)a) de la *Loi sur la défense nationale*, ou partie a) de son mandat. On trouvera plus de détails sur la première phase de l'examen dans le *Rapport annuel 2004-2005* de mon bureau.

En vertu de la partie a) de son mandat, le CST fournit deux types de renseignements étrangers à ses clients du gouvernement, notamment la GRC. La plupart de ses rapports portent sur des domaines d'intérêt général qui aident le client à s'acquitter des fonctions de son propre mandat. En plus de fournir ce type de soutien proactif, le CST offre un soutien réactif en répondant à des demandes de renseignements particulières que lui présentent ses clients.

#### Méthodologie

Le BCCST a examiné les activités du CST menées en vertu de la partie a) de son mandat pour appuyer la GRC pendant la période du 1<sup>er</sup> janvier au 31 décembre 2003. Il a reçu des réponses aux questions soumise tant verbalement que par écrit aux responsables du CST, ainsi que des brefs. Il a également reçu une liste des demandes de renseignements présentées au CST par la GRC et en a examiné plusieurs de manière approfondie. Lors de cet examen, les responsables du BCCST ont reçu deux démonstrations distinctes des activités à l'étude par le personnel du CST chargé directement des demandes.

<sup>17</sup> Le mandat du CST est défini à l'annexe E.

De plus, au cours de l'année, nous avons consacré beaucoup de temps et de ressources aux questions liées à l'interprétation des textes de loi, dont j'ai parlé en détail dans la section portant sur le contexte de l'examen.

## Examens effectués

Mon mandat d'examen général est défini à l'alinéa 273.63(2)a) de la *Loi sur la défense nationale*<sup>16</sup>. De plus, en vertu du paragraphe 273.65(8) de la *Loi*, je suis tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation ministérielle pour en contrôler la conformité, et de rendre compte du résultat de mon enquête au ministre.

Les autorisations ministérielles visant la collecte de renseignements étrangers sont accordées en vertu du paragraphe 273.65(1) de la *Loi sur la défense nationale*, tandis que les autorisations ministérielles visant les activités axées sur la sécurité des technologies de l'information sont accordées en vertu du paragraphe 273.65(3) de la *Loi*. Le BCCST procède à l'examen des activités du CST exercées sous le régime d'une autorisation ministérielle uniquement après que celle-ci est venue à échéance.

Pendant l'année 2006-2007, mon bureau a présenté au ministre quatre rapports d'examen classifiés, dont deux portaient sur les activités du CST exercées sous le régime d'une autorisation ministérielle – l'un sur la collecte des renseignements étrangers et l'autre sur la sécurité des technologies de l'information. Les deux autres examens ont été menés en vertu de mon mandat général, afin de contrôler la légalité des activités du CST.

<sup>16</sup> Les sections pertinentes de la *Loi sur la défense nationale* sont reproduites à l'annexe A.



## Examens indépendants du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST)

Au printemps 2006, deux examens indépendants portant sur la gestion de mon bureau ont été commandés. L'un portait sur l'administration, notamment la gestion et le contrôle des ressources financières, humaines et d'information, l'autre, sur les opérations. Dans ce dernier cas, il s'agissait d'évaluer si le bureau s'acquittait bien et efficacement des responsabilités confiées au commissaire dans le cadre de son mandat.

*J'ai été heureux de constater que les conclusions de ces examens administratifs étaient toutes positives.*

Les rapports de ces deux examens m'ont été remis au moment de ma nomination, ce qui m'a permis de profiter d'une évaluation indépendante de mon nouveau domaine de responsabilité. J'ai été heureux de constater que les conclusions de ces examens administratifs étaient toutes positives. Les recommandations issues de l'examen opérationnel ont fait l'objet d'une discussion approfondie lors d'un atelier qui a eu lieu le 21 août 2006 et qui était animé par les consultants responsables de l'examen. Des questions de méthodologie concernant l'examen opérationnel ont été soulevées, qui seront brièvement discutées plus loin dans ce rapport.

## Plan de travail

Un plan de travail triennal, mis à jour régulièrement, guide les activités de mon bureau. Pour faciliter l'établissement du calendrier, mon personnel consulte le CST sur les composantes d'examen du plan. Voici quelques exemples de critères qui déterminent leur choix des domaines qui seront soumis à un examen : les activités ou programmes du CST qui n'ont pas fait l'objet d'un examen par le passé ou récemment; les domaines recensés dans les briefings demandés au CST; la suite donnée aux recommandations issues des examens précédents; et les activités où les menaces à la vie privée sont jugées les plus élevées. Les membres de mon personnel, qui possèdent une connaissance détaillée des activités du CST, se posent des questions fondamentales comme les suivantes : qu'est-ce qui peut mal tourner? Quelles sont les probabilités que cela se concrétise? Le cas échéant, quelles seraient les répercussions?



Pour pouvoir procéder à un examen intégré des activités de sécurité nationales intégrées, le commissaire O'Connor a recommandé que des passerelles législatives soient établies entre la Commission indépendante d'examen des plaintes et des activités en matière de sécurité nationale visant la GRC qu'il propose de créer, le Comité de surveillance des activités de renseignement de sécurité et le Bureau du commissaire du CST afin de permettre l'échange d'information, le renvoi d'enquêtes à un autre organisme, la tenue d'enquêtes conjointes, ainsi que la coordination et la préparation des rapports<sup>12</sup>. Je suis favorable à cette proposition, bien qu'à ce jour l'absence de passerelle n'ait jamais été un obstacle opérationnel.

J'ai pris note avec satisfaction de l'observation suivante dans le rapport du juge O'Connor : « Je ne recommande pas d'élargir le mandat du CSARS au CST car je crois comprendre que le Bureau du commissaire du CST fonctionne très bien. Je ne vois donc aucune raison d'intervenir dans ses activités. »<sup>13</sup> J'ai également été heureux de constater que mon bureau avait été félicité pour la création en 2005-2006 de la Tribune des organismes d'examen<sup>14</sup>. Je reviendrai sur cette dernière un peu plus loin.

J'ai quelques réserves toutefois à propos de la recommandation du juge O'Connor de créer un comité de coordination pour l'examen intégré des questions de sécurité nationale<sup>15</sup>. Je crains en effet que la création d'un tel comité par voie législative – et la modification des lois connexes – n'introduise un niveau de bureaucratie superflu et improductif entre les organismes d'examen indépendants et le Parlement.

<sup>12</sup> Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, *Un nouveau mécanisme d'examen des activités de la GRC en matière de sécurité nationale* (Ottawa : Travaux publics et Services gouvernementaux Canada, 2006), p. 643.

<sup>13</sup> *Ibid.*, recommandation n° 11, p. 641.

<sup>14</sup> *Ibid.*, p. 316.

<sup>15</sup> *Ibid.*, recommandation n° 12, p. 654.

<sup>10</sup> *Ibid.*, recommandations nos 58 et 59, pp. 94-96.  
<sup>11</sup> *Ibid.*, pp. 93-95.

12 décembre 2006.

de l'enquête. Il a publié son rapport sur l'examen de la politique le 12 décembre 2006. L'honorable Dennis O'Connor a été nommé commissaire indépendant des activités de la GRC liées à la sécurité nationale (examen des recommandations sur la création d'un mécanisme d'examen canadiens relativement à Maher Arar (enquête sur les faits), ainsi que de le mandat d'enquêter et de faire rapport sur les actions des responsables relativement à Maher Arar a été mise sur pied le 5 février 2004. Elle a reçu La Commission d'enquête sur les actions des responsables canadiens

## Commission d'enquête O'Connor

serait bien placé pour procéder à cet examen<sup>11</sup>. 31 décembre 2011. Il a souligné que le comité de parlementaires proposé commencer au plus tard le 31 décembre 2010 et se terminer au plus tard le complet des dispositions et de l'application de la *Loi antiterroriste* devant Enfin, le Sous-comité a recommandé qu'on procède à un autre examen

précises sur le sujet lorsqu'un projet de loi sera déposé. position dans l'ensemble et je me propose de présenter des observations accès à des documents et renseignements classifiés. Je souscris à cette associés, notamment en ce qui a trait à la composition du comité et à son liées à la sécurité nationale, mais soulignait également les défis qui y sont appuyait l'idée d'un examen parlementaire plus dynamique des activités *antiterroriste*<sup>10</sup>. Dans son rapport annuel de l'an dernier, mon prédécesseur chargés de la sécurité nationale, avec les dispositions de la *Loi* renseignement de sécurité (SCRS) et le CST, et des éléments de la GRC certains ministères et organismes, tels que le Service canadien du le mandat de ce comité comprenne des vérifications de la conformité de déposé au Parlement à la première occasion. En outre, il a recommandé que *parlementaires sur la sécurité nationale*, ou une variante de celui-ci, soit projet de loi C-81 déposé pendant la 38<sup>e</sup> législature, *Loi sur le Comité de* Quant à l'examen et à la surveillance, le Sous-comité a recommandé que le

*des renseignements personnels.*

Je dois souligner que la méthode d'examen de mon bureau prévoit toujours un examen de conformité à la *Charte* et à la *Loi sur la protection*

# Recommandations du Sous-comité de la Chambre des communes

Dans son rapport final sur l'examen de la *Loi antiterroriste*, le Sous-comité de la Chambre a également traité de la question des autorisations ministérielles. J'ai été heureux de constater en particulier que le Sous-comité a mis en relief les observations de mon prédécesseur dans son rapport annuel 2005-2006 au sujet des ambiguïtés et imprécisions des dispositions de la loi à ce sujet, et des divergences entre mon bureau et le ministère de la Justice sur l'interprétation de ces dispositions. Sans formuler de recommandation particulière à ce sujet, le Sous-comité nous a néanmoins pressés, le conseiller juridique du gouvernement et moi-même, de régler cette question dans les meilleurs délais. Il a de plus demandé que le gouvernement précise, dans sa réponse au rapport final du Sous-comité et dans la mesure du possible, les points de désaccord et la façon dont ils ont été réglés. Si cela n'est pas fait, le Sous-comité est d'avis que je devrais fournir ces renseignements dans mon rapport annuel 2007-2008<sup>8</sup>. J'entends réexaminer cette recommandation quand viendra le temps de préparer ce rapport.

Le Sous-comité a également fait sienne la recommandation de la commissaire à la protection de la vie privée voulant que le paragraphe 273.65(8) de la *Loi sur la défense nationale* soit modifié de manière à ce que le commissaire du CST soit tenu d'examiner les activités d'interception de communications privées découlant d'une autorisation ministérielle, afin de s'assurer qu'elles respectent les exigences de la *Charte canadienne des droits et libertés* et de la *Loi sur la protection des renseignements personnels*, de même que l'autorisation elle-même. Cette position a été appuyée par une autre recommandation voulant que l'article 273.66 de la *Loi sur la défense nationale* soit modifié de manière à ce que le CST ne puisse entreprendre que des activités qui sont compatibles avec la *Charte canadienne des droits et libertés* et la *Loi sur la protection des renseignements personnels*, ainsi qu'avec les restrictions à l'exercice de son mandat déjà établies dans cet article<sup>9</sup>.

<sup>8</sup> Sous-comité sur la revue de la *Loi antiterroriste*, *Droits, restrictions et sécurité : un examen complet de la Loi antiterroriste et des questions connexes*. Rapport final du Comité permanent de la sécurité publique et nationale, mars 2007, p. 64.

<sup>9</sup> *Ibid.*, recommandations nos 44 et 45, pp. 63-64.

Dans le but de satisfaire aux principes de la reddition de comptes et de la transparence, le Comité a en outre recommandé que le ministre de la Défense nationale ou le CST soit tenu de rendre compte annuellement au Parlement du nombre d'autorisations ministérielles accordées au cours de l'année, du nombre d'autorisations encore en vigueur à la fin de l'année et du but général pour lequel chacune d'elles a été accordée (c'est-à-dire, pour l'obtention de renseignements étrangers ou pour la protection des systèmes ou réseaux informatiques)<sup>4</sup>.

La *Loi antiterroriste* a également modifié la *Loi sur les secrets officiels* et l'a rebaptisée *Loi sur la protection de l'information*. Cette loi établit le processus que les personnes astreintes au secret à perpétuité doivent suivre pour se prévaloir de la défense d'intérêt public en vue de la divulgation de renseignements classifiés. Le commissaire peut recevoir des renseignements classifiés dans le cadre de ce processus (voir l'annexe A). Or, la *Loi sur la protection de l'information* ne précise pas ce qu'il doit faire lorsque ces renseignements sont entre ses mains<sup>5</sup>. Le Comité a recommandé que le gouvernement précise la marche à suivre dans ce cas<sup>6</sup>. Je dois mentionner que mon bureau s'est doté de politiques et de procédures internes pour combler les lacunes cernées par le Comité.

Enfin, le Comité a discuté de la surveillance et de l'examen des dispositifs canadiens en matière de sécurité nationale et de lutte contre le terrorisme. Il a mentionné que notre bureau « est généralement perçu comme étant un mécanisme de surveillance efficace »<sup>7</sup>. Il a recommandé qu'un comité sénatorial permanent soit mis sur pied pour surveiller la législation antiterroriste et les dispositifs de sécurité nationale et qu'il rende compte périodiquement de ses conclusions. Le Comité a en outre recommandé que le Parlement procède à un examen approfondi des dispositions et de l'application de la *Loi antiterroriste* tous les cinq ans.

<sup>4</sup> *Ibid*, recommandation n° 20, p. 86.

<sup>5</sup> *Supra*, note 1, recommandation n° 26, p. 103.

<sup>7</sup> *Supra*, note 1, p. 128.

<sup>6</sup> À ce jour, je n'ai reçu aucun renseignement en vertu de la *Loi sur la protection de l'information*.



# Recommandations du Comité sénatorial spécial

Le Comité sénatorial spécial a présenté plusieurs recommandations concernant le CST, ainsi que le bureau du commissaire. En ce qui a trait au CST, le Comité s'est concentré sur les autorisations ministérielles et s'est dit d'accord avec les explications du CST quant aux raisons pour lesquelles l'organisme a besoin d'intercepter des communications privées dans le cadre de ses activités de collecte de renseignements étrangers et de protection de la sécurité des technologies de l'information. Il a également

accepté les explications du commissaire Lamer quant à la légitimité du recours à des autorisations ministérielles plutôt qu'à des autorisations judiciaires pour permettre l'interception de communications privées, étant donné que les mandats des tribunaux canadiens n'ont aucune

portée à l'extérieur du pays<sup>1</sup>. Le Comité était rassuré par le fait que notre bureau est tenu de vérifier la légalité des activités du CST, notamment l'interception de communications privées sous le régime d'une autorisation ministérielle. Il demeurait cependant préoccupé, tout comme le commissaire Lamer, par le manque de clarté de la norme requise pour convaincre le ministre que toutes les conditions nécessaires pour recourir à l'interception de communications privées étaient remplies. Le Comité a donc recommandé que les paragraphes 273.65(2) et (4) de la *Loi sur la défense nationale* soient modifiés de façon à préciser si ces conditions doivent être fondées sur une croyance raisonnable ou sur des soupçons raisonnables<sup>2</sup>. Il s'agit d'une question à laquelle mon bureau attache de l'importance et une clarification serait la bienvenue.

Comme le Comité souhaitait s'assurer que l'information interceptée était détruite s'il se révélait qu'elle n'était pas essentielle, ou lorsqu'elle n'était plus essentielle, il a recommandé que le CST élabore des politiques relatives à la conservation et à la destruction des renseignements, prévoyant notamment des délais précis pour l'élimination des renseignements interceptés, et qu'il rende ces politiques publiques<sup>3</sup>.

<sup>1</sup> Comité sénatorial spécial sur la *Loi antiterroriste, Justice fondamentale dans des temps exceptionnels : Rapport principal du Comité sénatorial spécial sur la Loi antiterroriste*, février 2007, p. 83.  
<sup>2</sup> *Ibid.*, recommandation n° 18, p. 85.  
<sup>3</sup> *Ibid.*, recommandation n° 19, p. 85.



Au fil du temps, le fossé ne cesse de se creuser entre les nouvelles technologies et les connaissances du grand public dans ce domaine. À plusieurs égards, les lois canadiennes n'ont pas non plus suivi le rythme de l'évolution technologique. Nous avons besoin d'une approche plus créative. À l'heure actuelle, des criminels et des terroristes sont passés maîtres de ces technologies complexes, car, contrairement aux institutions démocratiques, leur élan n'est pas freiné par des contraintes juridiques. Ceux qui participent au processus législatif doivent donc éviter de produire des lois visant les technologies du jour, qui seront vite dépassées. Nous devons plutôt veiller à ce que nos lois aient une portée assez large et soient structurées – par la réglementation ou autrement – de façon à pouvoir s'appliquer aux nouvelles technologies et ainsi à continuer de protéger à la fois notre vie privée et notre sécurité.

## Examen triennal de la Loi antiterroriste

La *Loi antiterroriste* a modifié entre autres la *Loi sur les secrets officiels* et la *Loi sur la défense nationale*. Les modifications apportées à cette dernière comportent notamment l'établissement d'un cadre législatif pour le CST et le commissaire du CST.

La *Loi antiterroriste* prévoyait la tenue d'un examen de ses dispositions et mené par un comité du Sénat ou de la Chambre des communes, ou un comité mixte, désigné ou mis sur pied à cette fin. Le Comité permanent de la sécurité publique et nationale de la Chambre a mis sur pied un sous-comité dans ce but à l'automne 2004. Parallèlement, le Sénat a également créé un comité spécial chargé de procéder à un examen approfondi de la *Loi*. Comme le mentionne le *Rapport annuel 2005-2006*, mon prédécesseur a comparu devant le Comité sénatorial spécial le 13 juin 2005 et, deux jours plus tard, devant le Sous-comité de la Chambre des communes. Le Comité sénatorial spécial a déposé son rapport le 22 février 2007, et le Sous-comité de la Chambre, le 27 mars 2007.

renseignements étrangers, a été une question particulièrement épineuse, étant donné l'absence de consensus sur l'interprétation de dispositions clés de la Loi.

D'un côté, mes prédécesseurs et moi avons reconnu l'importance des activités du CST, ainsi que les avantages que le gouvernement du Canada retire des renseignements étrangers qu'il lui fournit, notamment à une époque où la menace du terrorisme mondial n'a pas perdu de son intensité et où la sécurité de nos soldats en Afghanistan est toujours menacée.

De l'autre, nous avons soutenu sans équivoque, pendant nos mandats respectifs, que l'interprétation et les avis juridiques concernant les autorisations ministérielles fournis au CST par le ministère de la Justice ne sauraient s'appuyer sur une simple lecture des dispositions pertinentes de la partie V.1 de la *Loi sur la défense nationale*, et chacun d'entre nous en a informé le ministre de la Défense nationale en poste. De plus, mon prédécesseur immédiat, le très honorable Antonio Lamer, et moi-même avons tous les deux fait connaître nos positions aux personnes concernées au bureau du procureur général du Canada.

Au moment de déterminer si une activité est légale, je vérifie d'abord ce que la loi dit à ce sujet. La loi pertinente devient alors l'aune à laquelle on juge de la légalité de l'activité en cause. Il est difficile de le faire lorsque, dans des cas comme celui-ci, il existe des divergences d'opinion fondamentales sur ce que dit la loi.

Je ne mets pas en doute le rôle du ministère de la Justice dans l'élaboration de la loi et je ne vois pas non plus mon rôle de commissaire comme celui d'un arbitre dans son interprétation. Toutefois,

*La loi manque de clarté et elle doit être modifiée.*

comme je l'ai mentionné au ministre de la Défense nationale et au procureur général du Canada, la loi manque de clarté et elle doit être modifiée. C'est là un point de vue que partageaient également mes deux prédécesseurs. Cette question est à l'étude depuis un certain temps, et j'espère que le gouvernement procédera aux modifications requises à la première occasion. Je suis convaincu que la tâche ne sera pas trop lourde, car d'autres pays ont réussi à adopter et appliquent aujourd'hui des lois pour répondre à des exigences similaires.

rencontrer des spécialistes de la surveillance des activités de renseignement et de sécurité en provenance de 14 pays, dont le nôtre, et de discuter avec eux des défis communs que nous avons à relever à été une expérience remarquable. Je suis très heureux d'avoir pu participer à cette conférence, car cela m'a permis, à titre de nouveau commissaire du CST, de m'impregner de sujets d'intérêt mutuel en compagnie d'experts.

Dans les jours qui ont suivi ma nomination, j'ai rencontré le ministre de la Défense nationale et le chef du CST. J'ai en outre participé à de nombreuses séances d'information et visites, dont plusieurs au CST, et je tiens à remercier les responsables de leurs présentations détaillées. J'ai eu par la suite l'occasion de rencontrer d'autres hauts responsables du gouvernement fédéral, notamment la vérificatrice générale du Canada, la commissaire à la protection de la vie privée, les présidents du Comité de surveillance des activités de renseignement de sécurité (CSARS) et de la Commission des plaintes du public contre la GRC, ainsi que le sous-ministre et l'ombudsman de la Défense nationale.

Mais le plus important est le temps que j'ai consacré au travail de mon bureau et à me familiariser avec les activités et les préoccupations de mes prédécesseurs, ce dont je parlerai plus loin.

## CONTEXTE DE L'EXAMEN

Plusieurs éléments clés ont contribué à façonner le contexte dans lequel le bureau a effectué son travail au cours de l'année écoulée. Certains de ces éléments ont été décrits et commentés par mes prédécesseurs dans leurs rapports annuels. Dans le présent rapport, j'attirerai l'attention sur des éléments qui n'ont pas été abordés jusqu'à présent, ainsi que sur des faits nouveaux survenus dans les dossiers courants.

## Interprétation juridique

Depuis l'adoption de la *Loi antiterroriste* en décembre 2001, les personnes qui ont occupé le poste de commissaire du CST sont aux prises avec un dilemme persistant qui découle des modifications que cette loi omnibus a apportées à la *Loi sur la défense nationale*. La fonction d'examen du commissaire relative aux activités du CST menées sous le régime d'une autorisation ministérielle délivrée dans le seul but de recueillir des

Ce rapport est le premier que je présente à titre de commissaire du Centre de la sécurité des télécommunications (CST) depuis ma nomination à ce poste le 1<sup>er</sup> août 2006. Mon mandat est d'une durée de trois ans et se termine donc au mois d'août 2009.

Mon expérience professionnelle comprend 30 ans au sein de la magistrature. J'ai notamment été juge à la Cour suprême de 1989 à 2003. À mon avis, le rôle de juge et celui de commissaire du CST se rejoignent à plusieurs égards. En effet, un juge a pour souci premier de veiller à la tenue de procès équitables et de protéger les libertés individuelles, tout en préservant la paix et la sécurité. De même, la préoccupation fondamentale du commissaire du CST est de trouver un juste équilibre entre le droit à la protection des renseignements personnels et la nécessité d'obtenir des renseignements pour protéger la sécurité nationale. La loi reflète cette parenté de vocation en exigeant que le commissaire nommé à ce poste soit un juge surnuméraire ou un juge à la retraite d'une instance supérieure.

Dans les faits, toutefois, il existe une différence importante. Même si la question du secret se pose pour certaines actions en justice, le processus judiciaire est dans l'ensemble du domaine public. En revanche, le secret est au cœur même de la collecte des renseignements étrangers. Les principes d'équilibre sont néanmoins les mêmes. Je conçois le rôle de mon bureau comme étant de fournir à la population canadienne l'assurance que les activités cruciales du CST en matière de renseignement sont examinées avec soin par une autorité impartiale qui en vérifie la légalité et que ses droits sont protégés, sans compromettre le secret nécessaire à la protection de la sécurité nationale.

Au mois d'octobre 2006, j'ai eu l'occasion exceptionnelle de participer à la conférence internationale des organismes de surveillance du renseignement qui s'est déroulée au Cap, en Afrique du Sud. L'un des thèmes de la conférence portait sur le besoin de trouver un équilibre entre la protection des droits et libertés traditionnels des citoyens et la nécessité d'accroître les pouvoirs des autorités pour contre les menaces à la sécurité nationale. Le fait de pouvoir



Points saillants en 2006-2007 ( <i>suite</i> )	
• Examen des activités de collecte de renseignements électromagnétiques menées par le CST sous le régime d'une autorisation ministérielle / 18	
• Contexte / 18	
• Méthodologie / 19	
• Conclusions / 19	
• Aperçu des conclusions pour 2006-2007 / 19	
• Examens en cours / rapports à venir / 20	
• Plaintes relatives aux activités du CST / 20	
• Fonctions exercées en vertu de la Loi sur la protection de l'information / 20	
Bureau du commissaire / 21	
Regard sur l'avenir / 22	
• Commission d'enquête Major et Enquête interne Iacobucci / 22	
• Méthodologie de l'examen / 23	
Conclusion / 23	
Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications / 25	
Annexe B : Rapports classifiés, 1996-2007 / 27	
Annexe C : Etat des dépenses, 2006-2007 / 31	
Annexe D : Historique du Bureau du commissaire du Centre de la sécurité des télécommunications / 33	
Annexe E : Rôle et mandat du Centre de la sécurité des télécommunications / 35	



# TABLE DES MATIÈRES

Introduction / 1

Contexte de l'examen / 2

• Interprétation juridique / 2

• Retard des lois sur les progrès technologiques / 4

• Examen triennal de la *Loi antiterroriste* / 4

• Recommandations du Comité sénatorial spécial / 5

• Recommandations du Sous-comité de la Chambre des communes / 7

• Commission d'enquête O'Connor / 8

Rétrospective de l'année / 10

• Examens indépendants du BCCST / 10

• Plan de travail / 10

• Examens effectués / 11

Points saillants en 2006-2007 / 12

• Examen des activités de collecte de renseignements étrangers effectuées

par le CST à l'appui des activités de la GRC / 12

• Contexte / 12

• Méthodologie / 12

• Conclusions / 13

• Examen des activités liées à la protection de la sécurité des technologies de

l'information au sein d'un ministère / 14

• Contexte / 14

• Méthodologie / 15

• Conclusions / 15

• Examen des rôles des agents des relations avec la clientèle et

de la Section des politiques opérationnelles du CST dans la

divulgaration de renseignements personnels / 16

• Contexte / 16

• Méthodologie / 17

• Conclusions / 17



Commissaire du Centre de la  
sécurité des télécommunications

L'honorable Charles D. Gonthier, c.r.



Communications Security  
Establishment Commissioner

The Honourable Charles D. Gonthier, Q.C.

Mai 2007

Ministre de la Défense nationale  
Edifice MGen G.R. Pearkes, 13<sup>e</sup> étage  
101, promenade Colonel-By, tour nord  
Ottawa (Ontario)  
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63(3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous communiquer mon rapport annuel de 2006-2007 sur mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Charles D. Gonthier

P.O. Box/C.P. 1984, Station "B"/Succursale « B »  
Ottawa, Canada  
K1P 5R5  
(613) 992-3044 Téléc. : (613) 992-4096

Bureau du commissaire du Centre  
de la sécurité des télécommunications  
C.P. 1984,  
Succursale « B »  
Ottawa (Ontario)  
K1P 5R5

Tél. : (613) 992-3044

Télc. : (613) 992-4096

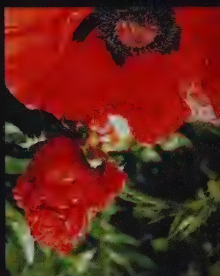
Site Web : <http://csec-ccst.gc.ca>

© Ministère des Travaux publics et des  
Services gouvernementaux Canada 2007  
ISBN 978-0-662-69804-3  
N° de cat. D95-2007

2006-2007



# Rapport annuel



COMMISSAIRE  
DU CENTRE  
DE LA SÉCURITÉ  
DES TÉLÉCOMMUNICATIONS



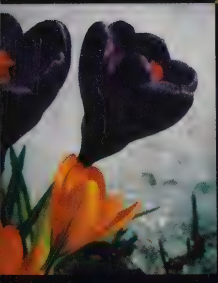


CA1  
ND800  
-S16



COMMUNICATIONS  
SECURITY  
ESTABLISHMENT  
COMMISSIONER

# Annual Report



2007-2008

Office of the Communications Security  
Establishment Commissioner  
P.O. Box 1984  
Station "B"  
Ottawa, Ontario  
K1P 5R5

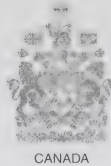
Tel.: (613) 992-3044  
Fax: (613) 992-4096  
Website: [www.ocsec-bccst.gc.ca](http://www.ocsec-bccst.gc.ca)

© Minister of Public Works and  
Government Services Canada 2008  
ISBN 978-0-662-05700-0  
Cat. No. D95-2008

Cover photos: Malak

  
**FSC**  
**Mixed Sources**  
Product group from well-managed  
forests and other controlled sources  
Cert no. SW-COC-000789  
[www.fsc.org](http://www.fsc.org)  
© 1996 Forest Stewardship Council

Communications Security  
Establishment Commissioner



Commissaire du Centre de la  
sécurité des télécommunications

The Honourable Charles D. Gonthier, C.C., Q.C.

L'honorable Charles D. Gonthier, C.C., c.r.

May 2008

Minister of National Defence  
MGen G.R. Pearkes Building, 13<sup>th</sup> Floor  
101 Colonel By Drive, North Tower  
Ottawa, Ontario  
K1A 0K2



Dear Sir:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my 2007–2008 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Charles D. Gonthier

P.O. Box/C.P. 1984, Station "B"/Succursale «B»  
Ottawa, Canada  
K1P 5R5  
(613) 992-3044 Fax: (613) 992-4096

*This report is dedicated to the memory of*

The Right Honourable Antonio Lamer  
P.C., C.C., C.D., LL.D., D.U.

1933–2007

---

## TABLE OF CONTENTS

Introduction /1

The Review Environment /2

- House of Commons Subcommittee and Special Senate Committee recommendations on the *Anti-terrorism Act* /2
- Proposed amendments to the *National Defence Act* /3
- Iacobucci Internal Inquiry and the Major Commission of Inquiry /6

The Year in Review /7

- Workplan /7
- Reviews undertaken of the activities of CSEC /9
- Methodology /10
- Overview of 2007–2008 findings /11

2007–2008 Review Highlights /13

- Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) /13
- Review of information technology security activities at a government department /14
- Review of CSEC's activities carried out under a ministerial directive /15
- Review of CSEC's counter-terrorism activities /17
- Review of CSEC's support to CSIS /18
- Reviews underway and planned /19
- Complaints about CSEC activities /20
- Duties under the *Security of Information Act* /20

The Commissioner's Office /20

A Tribute /22



---

Annex A: Mandate of the Communications Security Establishment  
Commissioner /23

Annex B: Classified Reports to the Minister, 1996–2008 /25

Annex C: Statement of Expenditures, 2007–2008 /29

Annex D: History of the Office of the Communications Security  
Establishment Commissioner (OCSEC) /31

Annex E: Role and Mandate of the Communications Security  
Establishment Canada (CSEC) /33

---

## INTRODUCTION

This is my second annual report as Communications Security Establishment Commissioner, and its publication occurs at the mid-point in my three-year term.

The fact that I am halfway through my first mandate gives me pause for reflection. Like my predecessors, I seek assurance of compliance with the spirit of the law, and not just the letter. In this regard, I am concerned with situations where lack of compliance with the law may arise, and I tailor my recommendations to safeguard against that possibility. If I determine there may not have been compliance with the law, I must of course inform the Minister of National Defence and the Attorney General of Canada.

*I seek assurance of compliance with the spirit of the law, and not just the letter.*

This leads me to contemplate one of my personal preoccupations—the role of the individual in doing the right thing. In the case of the Communications Security Establishment Canada (CSEC),<sup>1</sup> the people who are doing the work must have more than just technical ability. They must also have a fundamental respect for the rule of law and for democracy, which includes a reasonable expectation of privacy for all Canadians. CSEC's organizational culture must reflect these values, and CSEC must develop and follow policies and procedures that flow from the law and the values.

It is very clear to me that as a result of the terrorist acts of 2001, as well as subsequent terrorist activities, many Canadians continue to live with a heightened sense and level of risk, and there is little likelihood that these will diminish. This places a greater burden on people such as those employed at CSEC, because the government relies upon them to go beyond the mechanical aspects of information collection. They are called upon to reach for information that will support good decision making and thereby protect Canadians, but in a way that safeguards privacy.

---

<sup>1</sup> The name was changed to Communications Security Establishment Canada effective September 27, 2007, in order to comply with the Government of Canada's Federal Identity Program.

---

During the past year, I may at times have been critical of certain of CSEC's practices that, in my opinion, could be strengthened. I hold the view, however, that the striking point of the last several months has been the CSEC Chief's handling of an operational issue that came to light at the end of 2006 that had the potential for non-compliance. The Chief informed me about the matter at once, and has kept me apprised on a regular basis of all corrective steps taken. CSEC management's measured response addressed the needs of the organization, and was at the same time respectful of the people who serve in it, while leaving no doubt as regards their obligations.

## THE REVIEW ENVIRONMENT

### House of Commons Subcommittee and Special Senate Committee recommendations on the *Anti-terrorism Act*

In its Final Report presented to the House of Commons on March 27, 2007, the Subcommittee of the House of Commons reviewing the omnibus *Anti-terrorism Act* made a number of recommendations concerning CSEC and my office, dealing particularly with the legal ambiguities in the provisions allowing for ministerial authorizations. Since the *Anti-terrorism Act* received Royal Assent in December 2001, my predecessors and I have faced a persistent dilemma arising from the amendments this Act introduced to the *National Defence Act*. Particularly troublesome has been the lack of agreement between my office and CSEC concerning the legal advice provided to CSEC by the Department of Justice. At issue is the interpretation given to the provisions relating to ministerial authorizations.

The Subcommittee's Final Report urged government counsel and me to resolve the issues concerning ministerial authorizations. As well, the Subcommittee requested that the Government's response to the Final Report indicate, to the extent possible, what the issues of disagreement are and how they have been resolved. Failing this, the Subcommittee encouraged me to provide these details in my 2007–2008 Annual Report.

The Government issued its response on July 18, 2007. It noted that “CSE is working with Department of Justice officials to address these issues, with a view to bringing forward proposed legislative amendments in due course.”<sup>2</sup> One year later, there appears to have been a lack of progress. In the meantime, I wish to respond to the Subcommittee’s request and to describe two of my principal recommendations relating to ministerial authorizations.

*The Government noted that legislative amendments would be brought forward “in due course”. One year later, there appears to have been a lack of progress.*

## **Proposed amendments to the *National Defence Act***

The provision relating to ministerial authorizations issued for the sole purpose of obtaining foreign intelligence reads as follows:

### **Ministerial authorization**

**273.65** (1) The Minister may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.

### **Conditions for authorization**

- (2) The Minister may only issue an authorization under subsection (1) if satisfied that
  - (a) the interception will be directed at foreign entities located outside Canada;
  - (b) the information to be obtained could not reasonably be obtained by other means;

<sup>2</sup> *Response of the Government of Canada to the Final Report of the House of Commons Standing Committee on Public Safety and National Security Subcommittee on the review of the Anti-terrorism Act*, p. 20.



- 
- (c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
  - (d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

[...]

My first principal recommendation concerns the term *activity or class of activities* as it relates to CSEC and to the Commissioner. My predecessors and I have long held the view that a plain reading of the *National Defence Act* supports the interpretation that the interception authorized by the Minister is that of a private communication in relation to an *activity or class of activities* which is targeted or the object of inquiry, and not to a method of collection as contended by CSEC. Therefore, an important amendment would be to clarify the meaning of the term *activity or class of activities*.

My second principal recommendation is to define the terms *intercept* and *interception*, or to provide a reference to the existing definition of *intercept* in the *Criminal Code*. At present, these terms are not defined in the *National Defence Act*. However, they have both legal and operational significance for CSEC.

In the absence of definitions that are universally understood and consistently applied, it is difficult for me to interpret CSEC's legislated authority and to review how it has been applied.

The Special Senate Committee on the *Anti-terrorism Act* also made recommendations relating to ministerial authorizations. Notably, the Committee recommended "that subsections 273.65(2) and (4) of the *National Defence Act* be amended to clarify whether the facts and opinions, which are necessary to satisfy the Minister of National



---

Defence that all of the preconditions for issuing a written authorization to intercept private communications have been met, should be based on reasonable belief or reasonable suspicion”.<sup>3</sup> Clarifying in law the standard to be used remains an issue of interest to my office, and I continue to support making such an amendment to the *National Defence Act*.

In addition, I have made other recommendations to officials at CSEC and at the Department of Justice for amendments that I think would be worthwhile to enact.

In response to another recommendation of the House of Commons’ Subcommittee, the Government indicated that it did not intend to modify the *National Defence Act* to specify that my office should review interception activities for compliance with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*. As I pointed out in last year’s Annual Report, my office’s review methodology has always included an examination of compliance with all relevant laws, including the *Charter* and the *Privacy Act*.

The Subcommittee’s Final Report also recommended that the Government proceed with legislation to establish a National Security Committee of Parliamentarians responsible for the review of national security matters, and that this Committee be called upon to conduct a further comprehensive review of the *Anti-terrorism Act* after a fixed period. The Government responded that it has not determined if this is the best way to proceed. However, it went on to note that it “will propose an approach to national security review that will meet the basic objectives set out in the second report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar and is considering options for an enhanced role for Parliamentarians as a key

---

<sup>3</sup> Special Senate Committee on the *Anti-terrorism Act*, *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act*, February 2007, recommendation 18, p.78.

---

part of these proposals for an improved national security review framework.”<sup>4</sup> As I commented in my report last year, I concur with my predecessor’s position that welcomes “the prospect of more active parliamentary review of national security activities,” while also noting “challenges such as the composition of the committee and its access to classified information and documents.”<sup>5</sup>

## **Iacobucci Internal Inquiry and the Major Commission of Inquiry**

The Honourable Frank Iacobucci is in the process of conducting an internal inquiry into the actions of Canadian officials in relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin. He is to determine, amongst other matters, whether the detention or any mistreatment of these individuals in Syria or Egypt resulted, directly or indirectly, from actions of Canadian officials, particularly in relation to the sharing of information with foreign countries and, if so, whether those actions were deficient in the circumstances.

The Honourable John Major is conducting an inquiry into the investigation of the bombing of Air India Flight 182. In particular, he is to determine whether any changes in practice or legislation are required to prevent the recurrence of similar problems of cooperation between the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) in the investigation of terrorism offences, and to recommend how government should go about establishing a reliable and workable relationship between security intelligence and law enforcement agencies regarding the use of intelligence as evidence in a criminal trial.

I have an interest in the sharing of information about Canadians, particularly when that information is to be shared outside Canada. This is an area that my office continues to examine. In this context, the outcomes of the Iacobucci and Major Commissions may have an impact on security and intelligence agencies, as well as review agencies, including my office.

---

<sup>4</sup> *Supra*, note 2 at p. 25.

<sup>5</sup> Communications Security Establishment Commissioner, *Annual Report 2006–2007*, p. 8.

---

## THE YEAR IN REVIEW

Last year, I referred to the independent management review of the operations of my office, and to recommendations to improve our methodology. These matters have been thoroughly examined, and changes have been incorporated in new operational policies and procedures. My office has been implementing these changes in the conduct of reviews. One of the most notable is a new approach that involves examining processes which are common to several different CSEC activities. As a result, the review function is expected to be more effective in at least two ways: first, by avoiding a certain amount of duplication; and second, by creating a greater and readier understanding of underlying activities at the core of CSEC's mandate. CSEC has been kept informed throughout the process of implementing these changes, and specific issues of methodology that have a direct impact on that organization and on our working relationship have been discussed.

At my request, CSEC provided several briefings to my staff during the past year. Some of the briefings have become annual occurrences, such as those related to policy developments and updates, and also to the implementation of a new information management system. Other briefings have dealt with cyber-threat activities and with certain aspects of cooperation with CSIS. As is standard practice, and at our request, CSEC also provided briefings at the beginning of most reviews initiated during the year.

### Workplan

A three-year workplan guides the activities of my office. It is an integral component of the review process as well as being a focal point in the relationship between my office and CSEC. It is updated on a regular basis. Each update involves a re-assessment of the priority of planned and potential review projects and incorporates new information that may have come to our attention. For example, a review that has just been

---

completed may identify an area outside the scope of that review but which I believe needs to be examined further, perhaps to assess compliance with the law or to ensure the protection of the privacy of Canadians. In my report last year, I listed other criteria that contribute to determining what areas or topics will be included in the workplan. I must, however, always weigh what is reviewed against what is not, and be satisfied to the extent possible that those areas of greater risk to compliance with the law or to privacy are being examined.

CSEC is consulted on the workplan. There are several reasons for this. This is a standard practice in review to ensure that no one area of the organization is unduly burdened. There must be balance between my review mandate and CSEC's operational requirements mandated by the government. Another significant reason is that there is a need to ensure that the scheduling and scope of review projects is reasonable and can be carried out in a timely manner, taking into consideration the resources and mandates of both organizations.

An important initiative agreed upon by both CSEC and my office was to organize a roundtable discussion focussed on the working relationship. The objective was to optimize the review process, which as well means minimizing any adverse impact on the activities of CSEC. The meeting reviewed the business processes of both groups, identified points where improvement was desirable and proposed how to achieve those improvements. A number of issues related to the workplan were also identified and have been implemented. There was general agreement that this type of meeting was useful and served the interests of both organizations to keep open the lines of communication and to ensure that review works as intended.



---

## Reviews undertaken of the activities of CSEC

My general review mandate is set out in paragraph 273.63(2)(a) of the *National Defence Act*.<sup>6</sup> Under subsection 273.65(8) of the Act, I also have an obligation to review and report to the Minister as to whether the activities carried out under a ministerial authorization are authorized.

Ministerial authorizations for foreign intelligence collection are issued under the authority of subsection 273.65(1) of the *National Defence Act*, whereas ministerial authorizations for information technology security activities are issued under subsection 273.65(3) of the Act. My reviews of CSEC's activities conducted under ministerial authorizations are undertaken after the ministerial authorization has expired.

As I noted in my Annual Report last year: "The characteristics of contemporary communications technology mean that the interception of communications by CSE, directed at foreign entities outside Canada, runs the inherent risk of acquiring the private communications of Canadians. It is for this reason that a ministerial authorization is sought for this collection."<sup>7</sup>

The ministerial authorization provisions do not allow CSEC to target Canadian communications. However, "for the sole purpose of obtaining foreign intelligence"<sup>8</sup>, the Minister may authorize the interception of private communications of Canadians or persons in Canada as long as the interception was the result of CSEC's targeting a foreign entity located outside Canada. Ministerial authorizations for information technology security activities also authorize the interception of private communications that may be incidentally obtained by CSEC while protecting the systems and networks of a federal government department or agency.

---

<sup>6</sup> Please see Annex A for the text of the relevant sections of the *National Defence Act*.

<sup>7</sup> *Supra*, note 5 at p. 18.

<sup>8</sup> Subsection 273.65(1) of the *National Defence Act*.



---

Further, when collecting foreign intelligence, CSEC may also incidentally acquire information about Canadians. This information may only be retained if it is assessed as essential to the understanding of the foreign intelligence, and it may be included in foreign intelligence reporting if it is suppressed (i.e., replaced by a generic reference such as “a Canadian person”). When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC requires federal government departments and agencies to explain their authority to collect this information under their own respective mandates and to provide an operational justification of their need to know this information. If these conditions are met, CSEC may release the suppressed information. This year, two of my reports included detailed reviews of such releases.

During 2007–2008, my office submitted to the Minister five classified reports based on reviews completed during the year. Two of the reviews dealt with CSEC’s activities conducted under ministerial authorization; one of these pertained to foreign intelligence collection, while the other concerned information technology security. The other three reviews were conducted under my general mandate, to assess whether CSEC’s activities were in compliance with the law, and the extent to which it protected the privacy of Canadians in carrying out the activities.

## Methodology

Prior to beginning a review, my office provides CSEC with terms of reference that set out the objective, scope, criteria, a summary of the approach to be taken, and a timetable for the review. In conducting a review, OCSEC reviewers employ standard fact-finding tools and techniques to gather evidence, including examination of all relevant written and electronic records, and the associated authorities, policies and procedures. Reviewers also conduct extensive testing and sampling. Interviews are held with management and other personnel involved in the activities under review. Officials from other federal government departments and agencies may also be interviewed. In addition, legal

opinions and advice are examined. CSEC provides briefs and demonstrations of activities as well as answers to written questions. At the conclusion of the review process, reviewers meet with CSEC officials prior to finalizing their report. The purpose of this meeting is to outline review findings and conclusions.

## Overview of 2007–2008 findings

Although the five reviews reported on this year differed in subject, there were recurring themes, some of which are noted below. Overall, I am able to report that the activities of CSEC examined during the year complied with the law.

### Interpretation of ministerial authorizations

As noted earlier, CSEC and my office are still on opposite pages as regards the interpretation of the provisions of the *National Defence Act* relating to ministerial authorizations. However, pending legislative amendments, I have continued my predecessor’s practice of reviewing and reporting on whether CSEC’s activities conducted under ministerial authorization comply with the Act as it has been interpreted by the Department of Justice. On this basis, I am able to report that the two reviews of activities conducted under ministerial authorizations complied with the *National Defence Act* as interpreted by the Department of Justice.

### Information management

The theme of weak document and information management has been a consistent one over time. Good information management ensures that all relevant information and documentation is entered into the corporate record. However, as I and my predecessors have noted in previous reports, inadequate or missing information in CSEC’s corporate records can impair my ability to conduct reviews and to determine whether CSEC’s activities comply with the law. This has left me, in some instances, in a position of providing only a negative assurance to the Minister that I have no

*Inadequate information can impair my ability to conduct reviews.*

---

evidence of non-compliance with the law, rather than providing positive assurance, supported by evidence of compliance. CSEC is well aware of my concerns in this regard, is committed to addressing this issue, and is making progress in implementing a corporate records management system. CSEC is keeping me informed of its efforts. Future reviews will continue to seek documentation that demonstrates compliance with authorities, provides a record of all activities conducted, and confirms that supervisors are monitoring the performance of their staff.

### Interpretation of foreign intelligence mandate

In last year's Annual Report, I noted that one of the issues raised by my review of CSEC's foreign intelligence collection in support of the RCMP was "whether [the foreign intelligence part of CSEC's mandate] was the appropriate authority in all instances for CSE to provide intelligence support to the RCMP in the pursuit of its domestic criminal investigations."<sup>9</sup> Pending a re-examination of the legal issues raised, I decided that no assessment would be made of the lawfulness of CSEC's activities in support of the RCMP under the foreign intelligence part of CSEC's mandate as it is currently interpreted and applied. This issue remained unresolved as of March 31, 2008. My review of CSEC's support to CSIS, which is reported on below, raised similar issues. As I note in this instance, and unlike the matter of ministerial authorizations, I am in agreement with the advice that the Department of Justice has provided to CSEC. However, in certain cases, I question which part of CSEC's mandate should be used as the proper authority for conducting these activities. Discussions on these matters are ongoing.

---

<sup>9</sup> *Supra*, note 5 at p. 13.

---

## 2007-2008 REVIEW HIGHLIGHTS

### Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II)

#### Background

This report is the second and final phase of a review of certain foreign intelligence collection activities conducted under three ministerial authorizations that were in effect from March 2004 to December 2006. The first phase, which I reported on in last year's Annual Report, established an understanding of this foreign intelligence collection. It also examined the authorities, policies, procedures and management framework put in place to oversee the activities, and established the review criteria for this second phase.

The objective of this second phase was to assess and verify whether the activities that were authorized under the ministerial authorizations complied with the law as well as with the expectations set out in a ministerial directive relating to these activities.

#### Findings

With respect to the conditions imposed by the ministerial authorizations, which are articulated in subsection 273.65(2) of the *National Defence Act*, and the conditions imposed by the Minister as part of the authorization process, I found no evidence of non-compliance with the law. For a number of conditions, however, a lack of information and documentation did not allow my office to verify compliance. The review also found that, in some instances, CSEC had not complied with expectations set out in the ministerial directive, and I have so advised the Minister.



---

Operational policies were found to be in place and to provide direction to CSEC in the protection of the privacy of Canadians. No information was found to indicate that the actions of CSEC staff were in contravention of the operational policies. However, the absence and incompleteness of recorded information limits me to providing only a negative assurance to the Minister. That is to say that I have found no evidence of non-compliance with the law.

## Review of information technology security activities at a government department

### Background

This review examined information technology security activities conducted by CSEC under ministerial authorization in 2004–2005 at a government department. The objective was to assess compliance with the law and with the provisions of the ministerial authorization.

The *National Defence Act* mandates CSEC to help protect the Government of Canada's computer systems and networks by analyzing the vulnerability of selected computing and telecommunications systems and by providing information technology security advice and services to government departments and agencies.

CSEC's information technology security activities may result in the inadvertent interception of private communications of Canadians or personal information about a Canadian. For this reason, subsection 273.65(3) of the *National Defence Act* provides that:

The Minister may, for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the *Criminal Code*, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.



---

The CSEC Chief is responsible for seeking authorization on behalf of the department or agency requesting the activity to be covered. This ministerial authorization enables CSEC to undertake a complete security assessment of a department's networks.

## Findings

The review found that CSEC's information technology security activities at the department were in compliance with the law and with the ministerial authorization. The process by which CSEC acquired the ministerial authorization was in accordance with the requirements of the *National Defence Act* and the processes outlined in CSEC's related policies. It was also determined that the five conditions set out in subsection 273.65(4) of the Act were complied with satisfactorily. Measures were in place to protect the privacy of Canadians, and CSEC's use and retention of personal information about Canadians was found to comply with the law and CSEC policy.

## Review of CSEC's activities carried out under a ministerial directive

### Background

This review focused on certain activities undertaken by CSEC under a ministerial directive and, in the context of ministerial authorizations, in support of its foreign intelligence mandate articulated in paragraph 273.64(1)(a) of the *National Defence Act* for the period of April 1, 2005 to March 31, 2006.

Technology and telecommunications networks continue to increase in complexity. In order to fulfill its legislative mandate, CSEC conducts activities for the purposes of understanding the global information infrastructure and of locating foreign intelligence, in accordance with the intelligence priorities of the Government of Canada.

The objective of this review was to increase my office's knowledge of these activities and the authorities under which the activities are conducted. The review assessed CSEC's compliance with the ministerial directive and with the laws of Canada, including the *National Defence Act*, the *Charter*, and the *Privacy Act*, which governs the collection, use and disclosure of personal information. The review also assessed whether the activities conformed to CSEC's policies and procedures.

## Findings

This was my office's first examination of this activity, as governed by the ministerial directive. I am satisfied that CSEC takes measures to protect the privacy of Canadians in the use and retention of data obtained from this activity. However, I made a number of recommendations, as follows.

First, I believe that CSEC should re-examine its practice that only those private communications recognized by certain staff be accounted for.

I recommended that other staff that observe and handle private

*Staff that observe and handle private communications should be responsible for accounting for them.*

communications should also be responsible for accounting for them. Second, CSEC should re-assess which part of its legislative authority ought to be used to conduct certain of these activities, particularly those involving information provided by federal law

enforcement and security agencies. Finally, I also believe that CSEC should augment its policy and procedures in order to better guide and support these activities.

My office has since been advised that CSEC is re-examining these activities and associated policies and procedures. I support CSEC's initiative, and will continue to monitor the issues raised during this review.

---

## Review of CSEC's counter-terrorism activities

### Background

This review examined the lawfulness of CSEC's counter-terrorism activities in the period from April 1 to July 31, 2005.

In early October 2001, CSEC centralized foreign intelligence efforts as they relate to threats from international terrorism. The activities involve research and analysis of foreign intelligence data in order to identify terrorist targets and their operational and support networks. The information may be shared with federal government departments and agencies involved in intelligence and security-related matters, as well as with Canada's principal intelligence partners.

The main objectives of the review were to examine data collection and reports from the review period to verify that the information was collected, used and retained in compliance with the law, and to identify and report on any other issue of concern that might impact on the ability of CSEC to conduct its activities lawfully and to safeguard the privacy of Canadians.

### Findings

This review found that the activities conducted were in compliance with the law and with CSEC policy. Personnel who were interviewed during the course of this review were knowledgeable about the authorities governing their work. The report makes two recommendations. One would enhance accountability regarding linkages between CSEC reporting and the intelligence priorities of the Government of Canada, and the other would enhance accountability for the use and retention of private communications and information about Canadians.

---

## Review of CSEC's support to CSIS

### Background

The objective of this review was to assess the lawfulness of CSEC's activities in providing support to the Canadian Security Intelligence Service (CSIS) under CSEC's foreign intelligence mandate in the period from April 1, 2004 to March 31, 2005 and a sampling from November to December 2006.

CSEC provides regular foreign intelligence reporting to CSIS. Most of this reporting addresses general areas of interest that complement and support CSIS' own mandated responsibilities. CSEC also receives and responds to specific CSIS requests for intelligence-related information, provided that the requirement is consistent with documented Government of Canada intelligence priorities. A final aspect of CSEC's support to CSIS is that it responds to requests for the release of Canadian identities that have been suppressed in foreign intelligence reporting. Upon receipt of a formal request, CSEC must be satisfied with the justification and lawful authority for requiring the information.

### Findings

Overall, I am of the opinion that CSEC acted within its mandate in conducting activities in support of CSIS. I am in accord with the advice and guidance provided by the Department of Justice to CSEC respecting this support. However, in some cases, I question which part of CSEC's mandate should be used as the proper authority for conducting these activities and I have recommended that CSEC re-examine this matter. As of March 31, 2008, this was the subject of ongoing discussions between my officials and CSEC.

In addition, my office identified concerns respecting requests for the release of suppressed information, and respecting the CSIS-CSE Memorandum of Understanding of 1990 that guides the agencies' cooperation. Many of my findings reinforced those of two previous reviews of CSEC's foreign intelligence collection in support of the



---

RCMP and of the roles of CSEC's client relations officers and Operational Policy Section in the release of personal information, both of which are described in my 2006–2007 Annual Report.

I am pleased to note that since the period of review, CSEC continues to review its internal processes, policies and procedures, in order to make improvements in areas where deficiencies have been identified.

*CSEC continues to make improvements in areas where deficiencies have been identified.*

I have, however, recommended that CSEC re-visit the Memorandum of Understanding between CSIS and CSEC which is out of date and does not reflect current arrangements or practices between the two agencies. Given the international threat environment, it is my view that cooperation between security and intelligence agencies must be continually examined and the frameworks for cooperation kept up to date.

## Reviews underway and planned

My office has several reviews underway that I will be reporting on to the Minister in the coming year and will include in my next Annual Report. The subjects of these reviews include: activities conducted by CSEC under several foreign intelligence ministerial authorizations; the disclosure of information about Canadians to federal government departments and agencies; an examination of certain common practices of CSEC related to its mandated activities, and a comprehensive study of its information technology security activities. Some reviews that will begin in the next fiscal year will carry through to 2009–2010. Last year I indicated that I would be reporting on CSEC's use of technology to protect the privacy of Canadians. At fiscal year-end, this review was being finalized, and therefore it will be reported on in next year's Annual Report.



---

## Complaints about CSEC activities

My mandate includes undertaking any investigation I deem necessary in response to a complaint. During the 2007–2008 fiscal year my office received no complaints that warranted formal investigation.

## Duties under the *Security of Information Act*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy and seek to defend the release of classified information about CSEC on the grounds that it is in the public interest. No such matters were reported to my office in the 2007–2008 fiscal year.

## THE COMMISSIONER'S OFFICE

I continue to be supported in my work by a full-time staff of eight people, together with a number of subject matter experts who make themselves available, as required, under contract.

Keeping sufficiently current with technology to support my review of CSEC's activities is always a challenge. It was facilitated this year by CSEC itself. In the fall of 2007, CSEC opened its doors to members of my staff who attended two courses for CSEC employees, one respecting information technology security, and another course covering foreign intelligence.

In May 2007, I addressed a meeting of the Advisory Council on National Security that was held in Ottawa. The Advisory Council was created in April 2004 as a feature of the National Security Policy. It is made up of individuals from outside the government whose function is to provide advice on security matters.

---

Also in May, my office hosted a meeting of the Review Agencies Forum, which brings together the staff members of the Security Intelligence Review Committee, the Office of the Inspector General of the Canadian Security Intelligence Service, the Commission for Public Complaints against the Royal Canadian Mounted Police and my own office. The Forum provides an opportunity for review analysts to compare best practices and discuss issues of mutual interest and concern. In this regard, my office's review methodology initiative was discussed at length.

In June 2007, I had the pleasure of introducing U.S. Supreme Court Justice Antonin Scalia at the *International Conference on the Administration of Justice and National Security in Democracies*, held in Ottawa. The Conference, which was jointly sponsored by the Federal Court of Canada and the Canadian Centre of Intelligence and Security Studies at Carleton University, also provided me with an opportunity to renew my contacts with colleagues from other countries, some of whom I had met at the last *International Intelligence Review Agencies Conference (IIRAC)* in South Africa in October 2006.

Also in June, I was represented by the Executive Director at an international conference on Accountability of Intelligence and Security Agencies and Human Rights, held in The Hague under the auspices of the Dutch Review Committee on the Intelligence and Security Services and the Faculty of Law of Radboud University, Nijmegen. In September, I was represented by the Director of Operations at the annual conference of the Canadian Association for Security and Intelligence Studies in Calgary, where participants explored the many challenges facing the security and intelligence community.

Also in September, I attended a two-day conference entitled *Protecting Security and Human Rights: The Case for Migration in Canada* and sponsored by the Institute for Research in Public Policy.

All these initiatives demonstrate increasing interest, in Canada and abroad, in security and intelligence matters and their many dimensions.

---

Since its creation in 1996 by Order in Council pursuant to Part II of the *Inquiries Act*, the Office of the CSE Commissioner has been funded by the Department of National Defence, but has received administrative and other support from the Privy Council Office.

Over the fall months, a decision was taken that the long-standing relationship with the Privy Council Office would be severed, and that the administrative and other support activities for my office would be taken over by National Defence. I view this change in a positive light. I would be remiss, however, if I failed to take note of the outstanding help and support provided by the staff of the Privy Council Office over the last twelve years. Thank you from all of us.

In the interest of providing information about OCSEC's work, my office hosts a website ([www.ocsec-bccst.gc.ca](http://www.ocsec-bccst.gc.ca)) that describes our mandate and activities. In fiscal year 2007–2008, there were over 98,000 visits to the site, including visitors from approximately 40 countries outside North America.

In 2007–2008, my office's expenditures were \$1,220,999, which was well within budget for the period. Annex C to this report provides a summary of 2007–2008 expenditures.

## A TRIBUTE

On November 24, 2007, the Right Honourable Antonio Lamer, my predecessor as CSE Commissioner, died at age 74. Antonio Lamer was a renowned lawyer and jurist. He was appointed to the Supreme Court of Canada in 1980, and was named Chief Justice in 1990, a position that he occupied until his retirement in 2000.

For my part, he was my colleague on the bench for over 11 years, and my long-standing friend. His contribution to Canadian jurisprudence was outstanding, exceeded only by his love of Canada. He is missed.

---

## ANNEX A: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

### *National Defence Act – Part V.1*

- 273.63** (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.
- (2) The duties of the Commissioner are
- (a) to review the activities of the Establishment to ensure that they are in compliance with the law;
  - (b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and
  - (c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.
- (3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.
- (4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.
- (5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.



(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

**273.65** (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

### *Security of Information Act*

**15.** (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]

(5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]

(b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.



## **ANNEX B: CLASSIFIED REPORTS TO THE MINISTER, 1996–2008**

1. Principal vs. agent status – March 3, 1997 (TOP SECRET)
2. Operational policies with lawfulness implications – February 6, 1998 (SECRET)
3. CSE's activities under \*\*\* – March 5, 1998 (TOP SECRET Codeword/CEO)
4. Internal investigations and complaints – March 10, 1998 (SECRET)
5. CSE's activities under \*\*\* – December 10, 1998 (TOP SECRET/CEO)
6. On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)
7. How we test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)
8. A study of the \*\*\* collection program – November 19, 1999 (TOP SECRET Codeword/CEO)
9. On \*\*\* – December 8, 1999 (TOP SECRET/COMINT)
10. A study of CSE's \*\*\* reporting process — an overview (Phase I) – December 8, 1999 (SECRET/CEO)
11. A study of selection and \*\*\* — an overview – May 10, 2000 (TOP SECRET/CEO)
12. CSE's operational support activities under \*\*\* — follow-up – May 10, 2000 (TOP SECRET/CEO)
13. Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)
14. On findings of an external review of CSE's ITS program – June 15, 2000 (SECRET)
15. CSE's policy system review – September 13, 2000 (TOP SECRET/CEO)

16. A study of the \*\*\* reporting process — \*\*\* (Phase II) – April 6, 2001 (SECRET/CEO)
17. A study of the \*\*\* reporting process — \*\*\* (Phase III) – April 6, 2001 (SECRET/CEO)
18. CSE's participation \*\*\* – August 20, 2001 (TOP SECRET/CEO)
19. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – August 20, 2001 (TOP SECRET/CEO)
20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – August 21, 2002 (SECRET)
21. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – November 13, 2002 (TOP SECRET/CEO)
22. CSE's \*\*\* activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)
23. Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)
24. CSE's activities pursuant to \*\*\* Ministerial authorizations including \*\*\* – May 20, 2003 (SECRET)
25. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part I – November 6, 2003 (TOP SECRET/COMINT/CEO)
26. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part II – March 15, 2004 (TOP SECRET/COMINT/CEO)
27. A review of CSE's activities conducted under \*\*\* Ministerial authorization – March 19, 2004 (SECRET/CEO)
28. Internal investigations and complaints — follow-up – March 25, 2004 (TOP SECRET/CEO)

29. A review of CSE's activities conducted under 2002 \*\*\* Ministerial authorization – April 19, 2004 (SECRET/CEO)
30. Review of CSE \*\*\* operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)
31. CSE's support to \*\*\* – January 7, 2005 (TOP SECRET/COMINT/CEO)
32. External review of CSE's \*\*\* activities conducted under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)
33. A study of the \*\*\* collection program – March 15, 2005 (TOP SECRET/COMINT/CEO)
34. Report on the activities of CSE's \*\*\* – June 22, 2005 (TOP SECRET)
35. Interim report on CSE's \*\*\* operations conducted under Ministerial authorization – March 2, 2006 (TOP SECRET/COMINT)
36. External review of CSE \*\*\* activities conducted under Ministerial authorization – March 29, 2006 (TOP SECRET/CEO)
37. Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – June 16, 2006 (TOP SECRET/COMINT/CEO)
38. Review of information technology security activities at a government department under ministerial authorization – December 18, 2006 (TOP SECRET)
39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – February 20, 2007 (TOP SECRET/COMINT/CEO)
40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – March 31, 2007 (TOP SECRET/COMINT/CEO)
41. Review of information technology security activities at a government department under ministerial authorization – July 20, 2007 (TOP SECRET)

- 
42. Review of CSEC's counter-terrorism activities – October 16, 2007 (TOP SECRET/COMINT/CEO)
  43. Review of CSE's activities carried out under a ministerial directive – January 9, 2008 (TOP SECRET/COMINT/CEO)
  44. Review of CSEC's support to CSIS – January 16, 2008 (TOP SECRET/COMINT/CEO)
  45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – March 28, 2008 (TOP SECRET/COMINT/CEO)

---

## ANNEX C: STATEMENT OF EXPENDITURES, 2007–2008

### Standard Object Summary

Salaries and Wages	\$713,135
Transportation and Telecommunications	37,431
Information	21,239
Professional and Special Services	257,488
Rentals	151,894
Purchased Repair and Maintenance	3,538
Materials and Supplies	8,652
Acquisition of Machinery and Equipment	23,258
Other Expenditures	4,364
<b>Total</b>	<b>\$1,220,999</b>





---

## ANNEX D: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER (OCSEC)

The Office of the Communications Security Establishment Commissioner (OCSEC) was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Québec, who held the position until June 2003. He was succeeded by the Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., Chief Justice of Canada (retired) for a term of three years. The Honourable Charles D. Gonthier, C.C., Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act*. During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment Canada (CSEC) to determine whether they conformed with the laws of Canada; and to receive complaints about CSEC's activities.

Following the terrorist attacks in the United States on September 11, 2001, Parliament adopted the omnibus *Anti-terrorism Act* which came into force on December 24, 2001. The omnibus *Act* introduced amendments to the *National Defence Act*, by adding Part V.1 and creating legislative frameworks for both OCSEC and CSEC. It also gave the Commissioner new responsibilities to review activities carried out by CSEC under a ministerial authorization.

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act*. This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSEC on the grounds that it is in the public interest.

Under the Commissioner's current mandate, which entrenched in law the original mandate established in 1996 as well as the additional responsibilities described above, the Commissioner has retained the powers of a commissioner under Part II of the *Inquiries Act*.



---

## ANNEX E: ROLE AND MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

The Communications Security Establishment Canada (CSEC) is Canada's national cryptologic agency. Unique within Canada's security and intelligence community, CSEC employs code-makers and code-breakers to provide the Government of Canada with information technology security and foreign intelligence services. CSEC also provides technical and operational assistance to federal law enforcement and security agencies.

CSEC's foreign intelligence products and services support government decision-making in the fields of national security, national intelligence and foreign policy. CSEC's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSEC's information technology security products and services enable its clients (other government departments and agencies) to effectively secure their electronic information systems and networks. CSEC also conducts research and development on behalf of the Government of Canada in fields related to communications security.

CSEC has a three-part mandate under subsection 273.64(1) of the *National Defence Act*. These are known as parts (a) (b) and (c) of its mandate:

- (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
- (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
- (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.







# ANNEXÉ E : RÔLE ET MANDAT DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS CANADA (CSTC)

Le Centre de la sécurité des télécommunications Canada (CSTC) est l'organisme national de cryptologie du Canada. Organisme unique en son genre au sein de la collectivité canadienne de la sécurité et du renseignement, le CSTC emploie des cryptologues pour protéger la sécurité des technologies de l'information du gouvernement du Canada et lui fournir des renseignements étrangers. Il offre en outre une assistance technique et opérationnelle aux organismes fédéraux chargés de la sécurité et de l'application de la loi. Les produits et services de renseignement étranger du CSTC sont fournis à l'appui des décisions gouvernementales dans les domaines de la sécurité nationale, du renseignement national et de la politique étrangère. Ses activités en matière de renseignement électromagnétiques visent exclusivement des renseignements étrangers et sont assujetties aux priorités du gouvernement du Canada en matière de renseignement.

Dans le domaine de la sécurité des technologies de l'information, les produits et services du CSTC permettent à ses clients (les autres ministères et organismes gouvernementaux) d'assurer la sécurité de leurs systèmes et réseaux d'information électronique. Le CSTC effectue aussi des travaux de recherche-développement au nom du gouvernement du Canada dans des disciplines liées à la sécurité des télécommunications.

Le paragraphe 273.64(1) de la partie V.1 de la *Loi sur la défense nationale* établit le mandat du CSTC, qui comprend trois volets désignés sous le nom de parties a), b) et c) :

- a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
- b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;
- c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.



## ANNEXE D : HISTORIQUE DU BUREAU DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS (BCCST)

Le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) a été créé le 19 juin 1996, au moment de la nomination du premier commissaire, l'honorable Claude Bisson, O.C., ancien juge en chef du Québec. M. Bisson a occupé le poste de commissaire jusqu'en juin 2003. Le très honorable Antonio Lamer, c.p., C.C., c.d., L.L.D., d'u., juge en chef du Canada (à la retraite), lui a alors succédé pour un mandat de trois ans. L'honorable Charles D. Gonthier, C.C., c.r., qui a pris sa retraite de la Cour suprême du Canada en 2003, a été nommé commissaire en août 2006.

Pendant les six premières années de son mandat (de juin 1996 à décembre 2001), le commissaire a exercé ses fonctions conformément à plusieurs décrets, pris en vertu de la partie II de la *Loi sur les enquêtes*. Au cours de cette période, il a assumé une double responsabilité : examiner les activités du Centre de la sécurité des télécommunications Canada (CSTC) afin de déterminer si elles étaient en conformité avec les lois du Canada, et recevoir les plaintes relatives aux activités du CSTC.

Dans le sillage des attentats terroristes du 11 septembre 2001, le Parlement a adopté la *Loi antiterroriste omnibus*, qui a été promulguée le 24 décembre 2001. Cette loi modifie la *Loi sur la défense nationale*, en y ajoutant la partie V.1, qui établit le cadre législatif du BCCST et du CSTC, et elle confie au commissaire de nouvelles responsabilités relatives à l'examen des activités que mène le CSTC sous le régime d'une autorisation ministérielle.

En outre, la *Loi omnibus* a remplacé la *Loi sur les secrets officiels* par la *Loi sur la protection de l'information*, laquelle attribue au commissaire des fonctions précises pour les cas où une personne assermentée au secret à perpétuité souhaiterait invoquer la défense de l'intérêt public pour justifier la divulgation de renseignements classifiés sur le CSTC.

En vertu de son mandat actuel, qui inscrit dans la loi le mandat initial établi en 1996 ainsi que les nouvelles responsabilités supplémentaires décrites ci-dessus, le commissaire conserve tous les pouvoirs que confère à un commissaire la partie II de la *Loi sur les enquêtes*.





Sommaire des articles courants

Traitements et salaires	713 135 \$
Transports et télécommunications	37 431
Information	21 239
Services professionnels et spéciaux	257 488
Location	151 894
Achat de services de réparation et d'entretien	3 538
Fournitures et approvisionnements	8 652
Acquisition de machine et de matériel	23 258
Autres charges	4 364
Total	1 220 999 \$

- 
42. Review of CSSEC's counter-terrorism activities – 16 octobre 2007 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
43. Review of CSE's activities carried out under a ministerial directive – 9 janvier 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
44. Review of CSSEC's support to CSIS – 16 janvier 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
45. Review of CSSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – 28 mars 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
-

29. A review of CSE's activities conducted under 2002 \*\*\* Ministerial authorization – 19 avril 2004 (SECRET/Réserve aux Canadiens)
30. Review of CSE \*\*\* operations under Ministerial authorization – 1<sup>er</sup> juin 2004 (TRÈS SECRET/COMINT)
31. CSE's support to \*\*\* – 7 janvier 2005 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
32. External review of CSE's \*\*\* activities conducted under Ministerial authorization – 28 février 2005 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
33. A study of the \*\*\* collection program – 15 mars 2005 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
34. Report on the activities of CSE's \*\*\* – 22 juin 2005 (TRÈS SECRET)
35. Interim report on CSE's \*\*\* operations conducted under Ministerial authorization – 2 mars 2006 (TRÈS SECRET/COMINT)
36. External review of CSE's \*\*\* activities conducted under Ministerial authorization – 29 mars 2006 (TRÈS SECRET/Réserve aux Canadiens)
37. Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – 16 juin 2006 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
38. Review of information technology security activities at a government department under ministerial authorization – 18 décembre 2006 (TRÈS SECRET)
39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – 20 février 2007 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – 31 mars 2007 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
41. Review of information technology security activities at a government department under ministerial authorization – 20 juillet 2007 (TRÈS SECRET)

15. CSE's policy system review – 13 septembre 2000 (TRÈS SECRET/Réserve aux Canadiens)
16. A study of the \*\*\* reporting process — \*\*\* (Phase II) – 6 avril 2001 (SECRET/Réserve aux Canadiens)
17. A study of the \*\*\* reporting process — \*\*\* (Phase III) – 6 avril 2001 (SECRET/Réserve aux Canadiens)
18. CSE's participation \*\*\* – 20 août 2001 (TRÈS SECRET/Réserve aux Canadiens)
19. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – 20 août 2001 (TRÈS SECRET/Réserve aux Canadiens)
20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – 21 août 2002 (SECRET)
21. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – 13 novembre 2002 (TRÈS SECRET/Réserve aux Canadiens)
22. CSE's \*\*\* activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization – 27 novembre 2002 (TRÈS SECRET/Réserve aux Canadiens)
23. Lexicon of CSE definitions – 26 mars 2003 (TRÈS SECRET)
24. CSE's activities pursuant to \*\*\* Ministerial authorizations including \*\*\* – 20 mai 2003 (SECRET)
25. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part I – 6 novembre 2003 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
26. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part II – 15 mars 2004 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
27. A review of CSE's activities conducted under \*\*\* Ministerial authorization – 19 mars 2004 (SECRET/Réserve aux Canadiens)
28. Internal investigations and complaints — follow-up – 25 mars 2004 (TRÈS SECRET/Réserve aux Canadiens)

1. Principal vs. agent status – 3 mars 1997 (TRÈS SECRET)
2. Operational policies with lawfulness implications – 6 février 1998 (SECRET)
3. CSE's activities under \*\*\* – 5 mars 1998 (TRÈS SECRET Mot codé/Réserve aux Canadiens)
4. Internal investigations and complaints – 10 mars 1998 (SECRET)
5. CSE's activities under \*\*\* – 10 décembre 1998 (TRÈS SECRET/Réserve aux Canadiens)
6. On controlling communications security (COMSEC) material – 6 mai 1999 (TRÈS SECRET)
7. How we test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) – 14 juin 1999 (TRÈS SECRET Mot codé/Réserve aux Canadiens)
8. A study of the \*\*\* collection program – 19 novembre 1999 (TRÈS SECRET Mot codé/Réserve aux Canadiens)
9. On \*\*\* – 8 décembre 1999 (TRÈS SECRET/COMINT)
10. A study of CSE's \*\*\* reporting process — an overview (Phase I) – 8 décembre 1999 (SECRET/Réserve aux Canadiens)
11. A study of selection and \*\*\* — an overview – 10 mai 2000 (TRÈS SECRET/Réserve aux Canadiens)
12. CSE's operational support activities under \*\*\* — follow-up – 10 mai 2000 (TRÈS SECRET/Réserve aux Canadiens)
13. Internal investigations and complaints — follow-up – 10 mai 2000 (SECRET)
14. On findings of an external review of CSE's ITS program – 15 juin 2000 (SECRET)



- (7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.
- [...]
- 273.65** (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.
- Loi sur la protection de l'information*
- 15.** (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]
- (5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]
- b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession : [...]
- (ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.

# ANNEXE A : MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

## Loi sur la défense nationale – partie V.1

273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

- (2) Le commissaire a pour mandat
- a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;
  - b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;
  - c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de session de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

Le 24 novembre 2007, le très honorable Antonio Lamer, mon prédécesseur à titre de commissaire du CST, est décédé à l'âge de 74 ans. Avocat et juriste de renom, il avait été nommé à la Cour suprême du Canada en 1980, avant de devenir juge en chef en 1990, poste qu'il a occupé jusqu'à sa retraite en 2000.

Antonio Lamer a été mon collègue à la Cour pendant plus de 11 ans et mon ami de longue date. Il légue à la jurisprudence canadienne une contribution exceptionnelle, que seul surpasse son profond attachement au Canada. Il laisse un grand vide.

## HOMMAGE

En 2007-2008, les dépenses de mon bureau se sont chiffrées à 1 220 999 \$ et ont été largement couvertes par le budget approuvé pour cette période. On trouvera un résumé de ces dépenses à l'annexe C.

Un grand merci de la part de nous tous.

À l'automne, il a été décidé de mettre fin à la relation de longue date entre le BCCST et le Bureau du Conseil privé et de confier au ministère de la Défense nationale les fonctions de soutien administratif et autre de mon bureau. Ce changement me semble positif. Je m'en voudrais cependant de ne pas souligner l'aide et l'appui exceptionnels que nous avons reçus de l'équipe du Bureau du Conseil privé au cours des douze dernières années.

On peut trouver de l'information sur le BCCST en consultant le site Web ([www.ocsec-bccst.gc.ca](http://www.ocsec-bccst.gc.ca)), qui explique notre mandat et nos activités. Au cours de l'année financière 2007-2008, le site a reçu plus de 98 000 visites provenant notamment d'une quarantaine de pays à l'extérieur de l'Amérique du Nord.

Depuis sa création en 1996 par décret en vertu de la partie II de la Loi sur les enquêtes, le Bureau du commissaire du CST est financé par le ministère de la Défense nationale, mais il a reçu de l'aide et un soutien administratif du Bureau du Conseil privé.

À l'automne, il a été décidé de mettre fin à la relation de longue date entre le BCCST et le Bureau du Conseil privé et de confier au ministère de la Défense nationale les fonctions de soutien administratif et autre de mon bureau. Ce changement me semble positif. Je m'en voudrais cependant de ne pas souligner l'aide et l'appui exceptionnels que nous avons reçus de l'équipe du Bureau du Conseil privé au cours des douze dernières années.

En mai également, mon bureau a été l'hôte de la Tribune des organismes d'examen, qui a réuni les membres du Comité de surveillance des activités de renseignement de sécurité, du Bureau de l'Inspecteur général du Service canadien du renseignement de sécurité, de la Commission des plaintes du public contre la Gendarmerie royale du Canada et de mon propre bureau. La Tribune donne aux analystes chargés des examens l'occasion de comparer différentes pratiques optimales et de discuter de questions d'intérêt mutuel. À cet égard, la méthodologie d'examen de mon bureau a été discutée longuement.

En juin 2007, j'ai eu le plaisir de présenter le juge Antonin Scalia de la Cour suprême des États-Unis au Colloque international sur l'administration de la justice et la sécurité nationale dans les pays démocratiques, qui a eu lieu à Ottawa. Parrainé conjointement par la Cour fédérale du Canada et le Canadian Centre of Intelligence and Security Studies de l'Université Carleton, ce colloque m'a permis de renouer avec des collègues d'autres pays dont j'avais rencontré certains en octobre 2006 à la dernière Conférence internationale des organismes de surveillance du renseignement (IIRAC), en Afrique du Sud.

En juin toujours, la directrice exécutive de mon bureau m'a représenté à une conférence internationale sur la responsabilité des organismes du renseignement et de la sécurité et des droits de la personne, tenue à La Haye sous les auspices du comité néerlandais de surveillance des services du renseignement et de la sécurité et de la Faculté de droit de l'Université Radboud de Nîmègue. En septembre, le directeur des Opérations m'a représenté à la conférence annuelle de l'Association canadienne pour les études de renseignement et de sécurité, à Calgary, où les participants ont examiné les nombreux défis qui se posent dans les milieux du renseignement et de la sécurité.

En septembre, j'ai pris part à une conférence de deux jours intitulée « Protecting Security and Human Rights: The Case for Migration in Canada » et parrainée par l'Institut de recherche en politiques publiques. Toutes ces initiatives témoignent d'un intérêt grandissant, au Canada et à l'étranger, pour les questions de sécurité et du renseignement et leurs nombreuses dimensions.



## Plaintes relatives aux activités du CSTC

Dans le cadre de mon mandat, je dois procéder à toute enquête que je considère nécessaire par suite d'une plainte. Durant l'année financière 2007-2008, mon bureau n'a reçu aucune plainte ayant nécessité une enquête officielle.

### Fonctions exercées en vertu de la Loi sur la protection de l'information

La Loi sur la protection de l'information m'autorise à recevoir des renseignements de personnes astreintes au secret à perpétuité qui veulent se prévaloir de la défense « d'intérêt public » concernant la divulgation de renseignements classifiés relatifs au CSTC. Aucun problème de ce genre n'a été soumis à mon bureau en 2007-2008.

## LE BUREAU DU COMMISSAIRE

Je suis toujours secondé par un effectif de huit employés à temps plein et par un certain nombre d'experts contractuels auxquels nous faisons appel au besoin.

Un défi constant pour mon bureau est de rester au fait des technologies pour appuyer l'examen des activités du CSTC. Cette tâche a été simplifiée cette année par le Centre lui-même. À l'automne 2007, le Centre a ouvert ses portes aux membres de mon équipe qui ont suivi deux cours destinés à son personnel : un cours sur la sécurité des technologies de l'information et un autre sur le renseignement étranger.

En mai 2007, lors d'une réunion qui s'est tenue à Ottawa, j'ai entretenu les membres du Conseil consultatif sur la sécurité nationale, organisme créé en avril 2004 dans le cadre de la Politique de sécurité nationale. Formé de personnes extérieures au gouvernement, le Conseil a pour rôle de formuler des conseils sur des questions de sécurité.



opérationnelles du Centre relativement à la divulgation de renseignements personnels. Ces examens sont présentés dans mon rapport annuel de 2006-2007.

Je suis heureux de constater que, depuis la fin de la période d'examen, le Centre poursuit l'étude de ses processus, politiques et procédures internes dans l'intention d'apporter des améliorations là où des lacunes ont été signalées.

*Le CSTC continue d'apporter des améliorations là où des lacunes ont été signalées.*

J'ai cependant recommandé que le CSTC révise le protocole d'entente conclu avec le SCRS, qui n'est plus à jour et ne rend plus compte des arrangements ou pratiques actuels entre les deux organismes. Dans un contexte de menaces à l'échelle internationale, je suis d'avis que la coopération entre les organismes de sécurité et ceux du renseignement doit faire l'objet d'un examen continu et que les structures de collaboration doivent être revues périodiquement.

## Examens en cours ou projetés

Mon bureau a entamé plusieurs examens dont je rendrai compte au prochain rapport annuel. Entre autres sujets d'examen, mentionnons les activités effectuées par le CSTC en vertu de plusieurs autorisations ministérielles de collecte de renseignements étrangers; la divulgation de renseignements concernant des Canadiens à des ministères et organismes fédéraux; certaines pratiques du CSTC communes aux activités prévues par son mandat; et une étude exhaustive de ses activités liées à la sécurité des technologies de l'information. Certains examens engagés au cours du prochain exercice se poursuivront jusqu'en 2009-2010. L'an dernier, j'ai indiqué que je rendrais compte de l'usage par le CSTC de technologies pour protéger la vie privée des Canadiens. Au terme de l'exercice financier, cet examen était en voie d'être complet, et sera donc présenté dans le rapport annuel de l'an prochain.

Contexte

Cet examen portait sur la légalité des activités du CSTC lorsqu'il fournit une assistance au Service canadien du renseignement de sécurité (SCRS) en vertu du mandat en matière de renseignement étranger dévolu au CSTC, au cours de la période du 1<sup>er</sup> avril 2004 au 31 mars 2005, et comportait l'examen d'échantillons prélevés pour la période comprise entre novembre et décembre 2006.

Le CSTC transmet régulièrement des comptes rendus sur le renseignement étranger au SCRS. La plupart de ces rapports signalaient des points d'intérêt général qui complétaient et soutenaient les responsabilités qui incombent au SCRS. Le CSTC reçoit aussi certaines demandes d'information du SCRS liées au renseignement, et il y donne suite dans la mesure où elles cadrent avec les priorités du gouvernement du Canada en la matière. Un dernier aspect de l'assistance que le Centre prête au SCRS porte sur la divulgation de l'identité de Canadiens qui a été supprimée des rapports sur le renseignement étranger. Lorsqu'il reçoit une demande officielle à cet effet, le Centre doit déterminer que la justification est satisfaisante et être convaincu du droit légitime du demandeur.

Conclusions

Dans l'ensemble, je suis d'avis que le CSTC a respecté son mandat lorsqu'il a prêté assistance au SCRS. Je suis d'accord avec les conseils que le ministère de la Justice a offerts au Centre à ce sujet. Cependant, je questionne en vertu de quel volet de son mandat le CSTC peut s'acquitter de ces activités dans certains cas et j'ai recommandé au CSTC de réexaminer la question. Au 31 mars 2008, les pourparlers se poursuivaient entre mes représentants et le CSTC.

En outre, mon bureau a relevé des sources de préoccupation en ce qui concerne les demandes de divulgation de renseignements supprimés et le protocole d'entente de 1990 qui guide la collaboration entre le SCRS et le CSTC. Nombre de mes conclusions renforcent celles de deux examens antérieurs qui portaient sur la collecte de renseignements étrangers par le CSTC à l'appui de la GRC et sur les rôles exercés par les agents des relations avec la clientèle et la Section des politiques

## Contexte

Cet examen a porté sur la légalité des activités antiterroristes du CSTC au cours de la période du 1<sup>er</sup> avril au 31 juillet 2005.

Au début d'octobre 2001, le CSTC a centralisé les efforts déployés dans le domaine du renseignement étranger relativement aux menaces provenant du terrorisme international, et a procédé à la recherche et à l'analyse de données du renseignement étranger afin d'identifier les cibles terroristes et leurs réseaux d'opération et de soutien. Ces données peuvent être échangées avec les ministères et organismes fédéraux chargés du renseignement et de la sécurité, de même qu'avec les principaux partenaires du Canada en matière de renseignement.

L'objectif principal était d'examiner la collecte de données et les rapports préparés pendant la période d'examen pour vérifier que les renseignements ont été recueillis, utilisés et conservés de manière conforme à la loi, et pour relever et signaler toute autre source de préoccupation pouvant avoir une incidence sur l'aptitude du CSTC à mener à bien ses activités en toute légalité et à protéger la vie privée des Canadiens.

## Conclusions

Cet examen a permis de conclure que les activités exécutées étaient conformes à la loi ainsi qu'aux politiques du CSTC. Les membres du personnel interrogés étaient bien informés des instruments qui régissent leur travail. Le rapport renferme deux recommandations visant à renforcer la responsabilité du CSTC : d'une part, relativement aux liens entre les rapports préparés par le Centre et les priorités du gouvernement du Canada en matière de renseignement; d'autre part, relativement à l'utilisation et à la conservation des communications et des renseignements privés concernant des Canadiens.

L'examen avait pour objectif d'aider mon bureau à mieux comprendre ces activités et les autorisations sous-jacentes. Il a permis d'évaluer le respect des directives ministérielles et des lois du Canada par le CSTC, y compris la *Loi sur la défense nationale*, la *Charte* et la *Loi sur la protection des renseignements personnels* qui régit la collecte, l'utilisation et la divulgation de renseignements personnels. L'examen a aussi servi à évaluer dans quelle mesure les activités étaient conformes aux politiques et aux procédures du CSTC.

## Conclusions

C'était la première fois que mon bureau examinait ces activités mises en œuvre sous le régime d'une directive ministérielle. Je suis convaincu que le CSTC prend des mesures afin de protéger la vie privée des Canadiens lorsqu'il utilise et conserve les données découlant de ces activités. J'ai néanmoins formulé un certain nombre de recommandations présentées ci-après.

En premier lieu, j'estime que le CSTC devrait réexaminer sa pratique selon laquelle seules les communications privées reconnues par certains membres du personnel doivent faire l'objet d'un rapport. J'ai recommandé que d'autres employés qui observent et traitent des communications privées soient également tenus de rendre compte de ces communications. En second lieu, le CSTC devrait réévaluer de quel volet de son pouvoir législatif devrait relever certaines de ces activités, en particulier celles concernant des renseignements fournis par des organismes fédéraux chargés de l'application de la loi et de la sécurité. Enfin, je suis d'avis que le Centre devrait renforcer ses politiques et procédures afin de mieux orienter et soutenir ces activités.

Mon bureau a appris depuis lors que le CSTC réexamine ces activités ainsi que les politiques et procédures connexes. Je soutiens cette initiative, et j'entends maintenir un suivi des points soulevés durant cet examen.

*Les employés qui observent et traitent des communications privées devraient être tenus d'en rendre compte.*



Le chef du CSTC est tenu d'obtenir, pour le compte du ministère ou de l'organisme, l'autorisation visant l'activité demandée. Cette autorisation permet au CSTC de procéder à une évaluation complète de la sécurité des réseaux du ministère.

## Conclusions

L'examen a révélé que les activités du CSTC visant la sécurité des technologies de l'information dans le ministère étaient conformes à la loi et à l'autorisation ministérielle. Le processus d'obtention de l'autorisation ministérielle auquel a eu recours le CSTC respectait les dispositions de la *Loi sur la défense nationale* ainsi que les politiques connexes du Centre. Il a également été établi que les cinq conditions énoncées au paragraphe 273.65(4) de la *Loi* ont été respectées de manière satisfaisante. Des mesures étaient en place afin de protéger la vie privée des Canadiens, et l'utilisation et la conservation par le CSTC de renseignements personnels concernant des Canadiens étaient conformes à la loi et aux politiques de l'organisme.

## Examen des activités du CSTC exercées en vertu d'une directive ministérielle

### Contexte

Cet examen portait sur certaines activités entreprises par le CSTC en vertu d'une directive ministérielle et, dans le contexte d'autorisations ministérielles, à l'appui de son mandat de renseignement étranger énoncé à l'alinéa 273.64(1a) de la *Loi sur la défense nationale*, pour la période du 1<sup>er</sup> avril 2005 au 31 mars 2006.

La complexité des technologies et des réseaux de télécommunications ne cesse de s'accroître. Pour accomplir le mandat que lui confère la loi, le CSTC cherche à comprendre l'infrastructure mondiale de l'information et à localiser les renseignements étrangers, conformément aux priorités du gouvernement du Canada en matière de renseignement.



## Examen des activités liées à la sécurité des technologies de l'information au sein d'un ministère

### Contexte

Cet examen portait sur les activités liées à la sécurité des technologies de l'information menées par le CSTC au sein d'un ministère fédéral en vertu d'une autorisation ministérielle en 2004–2005. L'objectif était d'évaluer le respect de la loi ainsi que des dispositions de l'autorisation ministérielle.

Le CSTC est tenu, aux termes de la *Loi sur la défense nationale*, d'aider à protéger les systèmes et réseaux informatiques du gouvernement du Canada en analysant la vulnérabilité de certains systèmes informatiques et de télécommunication et en fournissant aux ministères et organismes gouvernementaux des conseils et des services touchant la sécurité des technologies de l'information.

Les activités du CSTC liées à la sécurité des technologies de l'information peuvent donner lieu à l'interception incidente de communications privées de Canadiens ou de renseignements personnels concernant un Canadien. Pour cette raison, voici ce qui est prévu au paragraphe 273.65(3) de la *Loi* :

Le ministre peut, dans le seul but de protéger les systèmes ou les réseaux informatiques du gouvernement du Canada de tout méfait ou de toute utilisation non autorisée ou de toute perturbation de leur fonctionnement, autoriser par écrit le Centre de la sécurité des télécommunications à intercepter, dans les cas visés à l'alinéa 184(2)c) du *Code criminel*, des communications privées qui sont liées à une activité ou une catégorie d'activités qu'il mentionne expressément.

## Examen des activités de collecte de renseignements électromagnétiques menées par le CSTC sous le régime d'une autorisation ministérielle (deuxième partie)

### Contexte

Ce rapport porte sur le second et dernier volet d'un examen de certaines activités de collecte de renseignements étrangers exécutées en vertu de trois autorisations ministérielles qui étaient en vigueur de mars 2004 à décembre 2006. La première partie, dont j'ai rendu compte dans le dernier *Rapport annuel*, a permis de comprendre cette activité du Centre. Elle a aussi servi à examiner les pouvoirs, les procédures et le cadre de gestion mis en place pour surveiller les activités, et à établir les critères d'examen de la deuxième partie.

L'objectif de la deuxième partie était d'évaluer et de vérifier si les activités effectuées aux termes des autorisations ministérielles respectaient la loi de même que les attentes énoncées dans une directive ministérielle connexe.

### Conclusions

En ce qui concerne les conditions imposées par les autorisations ministérielles, prescrites au paragraphe 273.65(2) de la *Loi sur la défense nationale*, et les conditions imposées par le ministre dans le cadre du processus d'autorisation, je n'ai relevé aucune preuve de non-conformité avec la loi. Cependant, faute d'information et de documentation, mon bureau n'a pas pu vérifier la conformité à un certain nombre de conditions. L'examen a aussi permis de constater que, dans certains cas, le CSTC n'avait pas respecté les attentes établies dans la directive ministérielle, et j'en ai informé le ministre.

<sup>9</sup> *Supra*, note 5, p. 13.

## Interprétation du mandat en matière de renseignement étranger

documents qui démontrent une conformité aux instruments habilitants, qui consistent toutes les activités effectuées et qui prouvent que les superviseurs font un suivi du rendement de leur personnel.

Dans le *Rapport annuel* de l'an dernier, j'ai indiqué qu'une des questions soulevées par mon examen de la collecte de renseignements étrangers par le CSTC à l'appui de la Gendarmerie royale du Canada était « de savoir si les demandes de renseignements de la GRC dans le cadre de ses enquêtes criminelles au pays relèvent [dans tous les cas du volet du mandat du CSTC concernant le renseignement étranger] »<sup>9</sup>. En attendant que les questions juridiques soulevées soient réexaminées, j'ai décidé qu'aucune évaluation ne serait faite de la légalité des activités d'assistance à la GRC, menées par le CSTC en vertu du volet de son mandat concernant le renseignement étranger, tel qu'il est interprété et appliqué en ce moment. Cette question n'était toujours pas réglée au 31 mars 2008. Mon examen de l'assistance que le CSTC prête au Service canadien du renseignement de sécurité, dont il est question ci-après, soulève des questions similaires. Comme je l'indique en l'occurrence, et contrairement à la question des autorisations ministérielles, je suis d'accord avec le conseil que le ministère de la Justice a fourni au CSTC. Toutefois, dans certains cas, je questionne en vertu de quel volet de son mandat le CSTC peut s'acquitter de ces activités. Mon équipe continue d'approfondir la question avec le CSTC.

Même si les cinq examens de l'année portaient sur des sujets différents, on note des thèmes récurrents, dont certains sont décrits ci-dessous. Dans l'ensemble, je peux constater que les activités du CSTC examinées au cours de l'année étaient conformes à la loi.

## **Interprétation des autorisations ministérielles**

Comme je l'ai mentionné, le CSTC et mon bureau ne s'entendent toujours pas quant à l'interprétation des dispositions de la *Loi sur la défense nationale* relatives aux autorisations ministérielles. Cependant, d'ici l'adoption d'amendements législatifs, j'ai repris la pratique de mon prédécesseur, qui consiste à examiner si les activités du CSTC exécutées en vertu d'une autorisation ministérielle cadrent avec la *Loi* telle qu'elle a été interprétée par le ministère de la Justice, et à en rendre compte. Dans cette optique, je peux constater que les deux examens menés sur des activités découlant d'une autorisation ministérielle étaient conformes à la loi telle qu'elle est interprétée par le ministère de la Justice.

## **Gestion de l'information**

Un thème qui revient régulièrement concerne des lacunes dans la gestion des documents et de l'information. Si l'information est correctement gérée, tous les renseignements et documents pertinents figurent dans les dossiers de l'organisation. Or, comme mes prédécesseurs et moi-même l'avons indiqué dans les rapports antérieurs, des renseignements inadéquats ou manquants dans les dossiers du CSTC peuvent

entraver ma capacité d'effectuer des examens et d'établir si l'organisme a agi en conformité avec la loi. Par conséquent, il s'ensuit, là où je l'indique, que je ne puisse offrir au ministre que l'assurance négative que je n'ai aucune preuve de non-respect de la loi, à défaut d'une assurance positive qui s'appuierait sur une preuve de légalité. Le CSTC est tout à fait au courant de mes préoccupations à cet égard, il est résolu à trouver des solutions et il est en voie de mettre en œuvre un système de gestion des dossiers. Il me tient au courant de ses mesures en ce sens. À l'avenir, nos examens continueront à chercher des

*Des renseignements inadéquats peuvent entraver ma capacité d'effectuer des examens.*



## Méthodologie

Avant de commencer un examen, mon bureau fournit au CSTC un cadre de référence dans lequel sont énoncés l'objectif, la portée et les critères de l'examen, et qui renferme un résumé de l'approche à adopter et un calendrier d'exécution. Durant un examen, les examinateurs du BCCST emploient des outils et des techniques standard de recherche des faits pour recueillir des éléments de preuve, ce qui comprend l'examen de tous les documents imprimés et électroniques pertinents ainsi que des autorisations, politiques et procédures connexes. Les examinateurs effectuent aussi de nombreux essais ainsi que des prises d'échantillons. Ils procèdent à des entrevues avec les gestionnaires et les autres intervenants qui ont participé aux activités à l'étude. Ils peuvent également interroger des représentants d'autres ministères et organismes fédéraux. En outre, les opinions et avis juridiques sont examinés. Le CSTC donne des séances d'information et des démonstrations d'activités, et répond à des questions écrites. Au terme du processus, les examinateurs rencontrent les représentants du Centre pour passer en revue les constatations et conclusions de l'examen avant de mettre la dernière main à leur rapport.

durant l'exercice 2007-2008, mon bureau a remis au ministre cinq rapports classifiés basés sur des examens complétés au courant de l'année. Deux examens visaient des activités du CSTC menées en vertu d'une autorisation ministérielle, dont l'une portait sur la collecte de renseignements étrangers, et l'autre sur la sécurité des technologies de l'information. Les trois autres examens ont été réalisés en vertu de mon mandat général, soit d'évaluer si les activités du CSTC sont conformes à la loi et dans quelle mesure l'organisme protège la vie privée des Canadiens dans l'exécution de ses activités.

vertu de leurs mandats respectifs et qu'ils fournissent une justification opérationnelle de leur besoin de connaître cette information. Si ces conditions sont réunies, le Centre peut divulguer les renseignements supprimés. Cette année, deux de mes rapports comportaient des examens détaillés de ce genre de divulgation.



<sup>8</sup> Paragraphe 273.65(1) de la *Loi sur la défense nationale*.

<sup>7</sup> *Supra*, note 5, p. 18.

Les autorisations ministérielles pour la collecte de renseignements étrangers sont accordées en vertu du paragraphe 273.65(1) de la *Loi*, tandis que celles relatives à la sécurité des technologies de l'information le sont aux termes du paragraphe 273.65(3) de la *Loi*. J'entame mes examens des activités du CSTC découlant d'autorisations ministérielles après l'expiration de l'autorisation ministérielle.

Comme je l'ai mentionné dans mon dernier rapport annuel, « [c]ompte tenu des caractéristiques des technologies de communication modernes, le CSTC court le risque inhérent, lorsqu'il tente d'intercepter les communications d'entités qui se trouvent à l'étranger, d'intercepter en même temps des communications privées de Canadiens. C'est pourquoi il doit obtenir une autorisation ministérielle à cette fin »<sup>7</sup>.

Les dispositions de l'autorisation ministérielle ne permettent pas au CSTC de cibler les communications de Canadiens. Cependant, en vertu de la *Loi sur la défense nationale*, le ministre peut, « dans le seul but d'obtenir des renseignements étrangers »<sup>8</sup>, autoriser le Centre à intercepter des communications privées de Canadiens et de personnes au Canada dans la mesure où l'interception vise une entité étrangère située à l'extérieur du Canada. Les autorisations ministérielles relatives à la sécurité des technologies de l'information permettent aussi l'interception incidente de communications privées que le Centre peut capter alors qu'il assure la protection des systèmes et réseaux d'un ministère ou organisme fédéral.

De plus, lorsqu'il recueille des renseignements étrangers, le CSTC peut incidemment acquérir des renseignements personnels sur des Canadiens. Il peut conserver ces renseignements uniquement s'il les juge indispensables à la compréhension du renseignement étranger et peut les inclure dans ses rapports sur le renseignement étranger pour autant qu'ils soient supprimés (c'est-à-dire remplacés par une référence générique telle que « un Canadien »). Quand, par la suite, des ministères ou organismes fédéraux demandent au CSTC de divulguer des renseignements supprimés, le Centre exige qu'ils justifient leur droit de recueillir ces renseignements en

<sup>6</sup> Se reporter à l'annexe A pour le libellé des articles pertinents de la Loi sur la défense nationale.

## Examens relatifs aux activités du CSTC

critères qui influent sur le choix des sujets inscrits au plan de travail. Cependant, je dois toujours évaluer l'importance relative des différentes questions pouvant faire l'objet d'un examen et être convaincu, dans la mesure du possible, que celles qui présentent les plus grands risques sur le plan du respect de la loi ou de la protection de la vie privée sont soumises à un examen.

Le CSTC est invité à donner son avis sur le plan de travail, et ce, pour plusieurs raisons : il est pratique courante de faire en sorte qu'aucun secteur de l'organisation ne soit soumis à une charge d'examen excessive; il doit y avoir un équilibre entre mon mandat d'examen et les obligations opérationnelles imposées au Centre par le gouvernement. En outre, il est important de voir à ce que l'échelonnement et la portée des projets d'examen soient raisonnables et à ce que ces projets soient réalisables dans des délais opportuns, compte tenu des ressources et des mandats des deux organismes.

Le CSTC et mon bureau ont pris l'initiative importante de tenir une table ronde sur nos relations de travail. L'objectif visé était d'optimiser le processus d'examen, afin notamment d'atténuer tout effet négatif sur les activités du Centre. La rencontre a permis de passer en revue les processus administratifs de part et d'autre, de s'entendre sur des points à améliorer et de proposer des moyens à cet effet. Des mesures ont été prises à la suite de questions soulevées au sujet du plan de travail. De l'avis général, ce genre de réunion a été utile et a contribué aux objectifs des deux organismes de maintenir des voies de communication ouvertes et de faire en sorte que les travaux d'examen donnent les résultats escomptés.

Mon mandat général d'examen est énoncé à l'alinéa 273.63(2)a) de la Loi *sur la défense nationale*<sup>6</sup>. En vertu du paragraphe 273.65(8) de la Loi, je suis en outre tenu de vérifier si les activités découlant d'une autorisation ministérielle sont autorisées et d'en rendre compte au ministre.

L'an dernier, j'ai mentionné l'examen indépendant portant sur la gestion de mon bureau et les recommandations visant à améliorer nos méthodes. Après une étude approfondie, nous avons adopté des changements dans nos nouvelles politiques et procédures opérationnelles, et mon bureau les applique dans le cadre des examens. Un des plus notables est une nouvelle méthode qui porte sur l'examen des processus communs à plusieurs activités du CSTC. Elle devrait rendre la fonction d'examen plus efficace, au moins sur deux plans : en premier lieu, en évitant certaines répétitions; et en second lieu, en favorisant une compréhension plus complète et plus directe des activités au cœur du mandat du Centre. Celui-ci a été tenu au courant tout au long de la mise en œuvre de ces changements, et des questions précises de méthodologie ayant une incidence directe sur le Centre et sur nos relations de travail ont été discutées.

À ma demande, le CSTC a présenté plusieurs brefs brefs à mon équipe. Certains sont devenus des événements annuels, comme les séances ayant trait à l'élaboration et à la mise à jour des politiques ou à la mise en œuvre d'un nouveau système de gestion de l'information. D'autres portaient sur les cybermenaces et certains aspects de la coopération avec le SCRS. À notre demande et conformément aux pratiques en vigueur, le CSTC nous a aussi donné des séances d'information au début de la plupart des examens entamés durant l'année.

## Plan de travail

Un plan de travail triennal guide les activités de mon bureau. Ce plan, qui est revu régulièrement, fait partie intégrante du processus d'examen et constitue un pivot de la relation entre mon bureau et le CSTC. Chacune de ses mises à jour comporte une réévaluation de l'ordre de priorité des projets d'examen prévus ou possibles et prend en compte les nouveaux renseignements dont nous avons connaissance. Ainsi, un examen qui vient de se terminer peut faire ressortir un aspect qui dépasse la portée de l'examen même mais que j'estime utile d'approfondir, par exemple pour évaluer la conformité avec la loi ou assurer la protection de la vie privée des Canadiens. Dans mon rapport de l'an dernier, j'ai fait état d'autres

## L'enquête interne Iacobucci et la Commission d'enquête Major

L'honorable Frank Iacobucci a entamé une enquête interne concernant les agissements des responsables canadiens relativement à Abdullah Almaliki, Ahmad Abou-Elmaati et Muayyed Nureddin. Il doit déterminer, entre autres choses, si la détention ou tout mauvais traitement de ces personnes en Syrie ou en Egypte découle, directement ou indirectement, des actions de responsables canadiens, particulièrement en ce qui concerne l'échange de renseignements avec des pays étrangers et, le cas échéant, si ces actions comportaient des lacunes dans les circonstances.

L'honorable John Major fait enquête sur les mesures d'investigation prises à la suite de l'attentat à la bombe contre le vol 182 d'Air India. Il doit notamment établir si des changements de pratique ou législatifs s'imposent pour éviter d'autres problèmes similaires de coopération entre le Service canadien du renseignement de sécurité (SCRS) et la Gendarmerie royale du Canada (GRC), dans le cadre des enquêtes relatives à des infractions de terrorisme. Il doit également recommander au gouvernement des moyens d'établir une relation fiable et fonctionnelle entre les organismes du renseignement de sécurité et les organismes d'exécution de la loi relativement à l'utilisation du renseignement comme élément de preuve dans un procès criminel.

Je m'intéresse à l'échange de données concernant les Canadiens, particulièrement lorsque ces renseignements doivent être échangés à l'extérieur du Canada. C'est une question que mon bureau continue d'examiner. À cet égard, les conclusions des commissions Iacobucci et Major pourraient avoir une incidence sur les organismes du renseignement et de la sécurité, ainsi que sur les organismes d'examen, y compris mon bureau.



La clarification dans la *Loi* de la norme à appliquer demeure une question à l'ordre du jour pour mon bureau, et je continue d'appuyer un tel amendement à la *Loi sur la défense nationale*.

Par ailleurs, j'ai recommandé aux représentants du CSTC et du ministère de la Justice d'autres modifications que je juge pertinentes.

En réponse à une autre recommandation du Sous-comité de la Chambre des communes, le gouvernement a fait savoir qu'il n'a pas l'intention de modifier la *Loi* afin de préciser que mon bureau devrait procéder à des examens des activités liées à l'interception pour déterminer si elles sont conformes à la *Charte canadienne des droits et libertés* et à la *Loi sur la protection des renseignements personnels*. Comme je l'ai signalé dans mon rapport annuel de l'an dernier, la méthode d'examen de mon bureau a toujours intégré une vérification de la conformité par rapport à toutes les lois pertinentes, y compris la *Charte* et la *Loi sur la protection des renseignements personnels*.

Le Sous-comité recommandait également dans son rapport final que le gouvernement établisse par voie législative un comité de parlementaires qui serait chargé d'examiner les questions de sécurité nationale et que ce comité soumette la *Loi antiterroriste* à un autre examen exhaustif à l'issue d'une période déterminée. Le gouvernement a répondu qu'il n'a pas décidé si telle était la meilleure façon de procéder. Il a toutefois indiqué qu'il « proposera une approche visant la sécurité nationale qui remplira les objectifs de base énoncés dans le deuxième rapport de la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar; il étudie aussi des options pour accroître le rôle des parlementaires en tant qu'élément clé des propositions visant à mettre en place un meilleur cadre d'examen des mesures de sécurité nationale »<sup>4</sup>. Comme je l'ai indiqué dans mon rapport de l'an dernier, je suis d'accord avec mon prédécesseur qui a dit appuyer « l'idée d'un examen parlementaire plus dynamique des activités liées à la sécurité nationale », mais en soulignant « les défis qui y sont associés, notamment en ce qui a trait à la composition du comité et à son accès à des documents et renseignements classifiés »<sup>5</sup>.

<sup>4</sup> *Supra*, note 2, p. 28.

<sup>5</sup> Commissaire du Centre de la sécurité des télécommunications, *Rapport annuel 2006-2007*, p. 8.



février 2007, recommandation n° 18, p. 85.

CSTC et d'examiner la façon dont ils ont été appliqués.

Ma seconde recommandation principale est de définir les termes

Ma première recommandation principale concerne l'expression *activité*

$$[\dots]$$

la défense ou à la sécurité.

que si elles sont essentielles aux affaires internationales, à

privée des Canadiens et pour faire en sorte que les

(d) il existe des mesures satisfaisantes pour protéger la vie

obtenir grâce à l'interception justifie l'interception envisagée,

c) la valeur des renseignements étrangers que l'on espère

Le gouvernement a indiqué que des modifications législatives seraient adoptées en temps opportun. Un an plus tard, il semble y avoir eu peu de progrès.

Le gouvernement a publié sa réponse le 18 juillet 2007, dans lequel il indique que « le CST collabore avec les fonctionnaires du ministère de la Justice afin de [...] régler [ces questions] et de faire adopter les modifications législatives proposées en temps opportun ». Un an plus tard, il semble y avoir eu peu de progrès. En attendant que les choses évoluent, j'acquiesce à la demande du Sous-comité et j'explique deux de mes principales recommandations concernant les autorisations ministérielles.

## Modifications proposées à la Loi sur la défense nationale

La disposition relative aux autorisations ministérielles accordées aux seules fins de l'obtention du renseignement étranger est la suivante :

### Autorisation ministérielle

**273.65** (1) Le ministre peut, dans le seul but d'obtenir des renseignements étrangers, autoriser par écrit le Centre de la sécurité des télécommunications à intercepter des communications privées liées à une activité ou une catégorie d'activités qu'il mentionne expressément.

### Conditions d'autorisation

- (2) Le ministre ne peut donner une autorisation que s'il est convaincu que les conditions suivantes sont réunies :
- a) l'interception vise des entités étrangères situées à l'extérieur du Canada;
  - b) les renseignements à obtenir ne peuvent raisonnablement être obtenus d'une autre manière;

<sup>2</sup> Réponse du gouvernement du Canada au Rapport final du Sous-comité sur la revue de la Loi antiterroriste, du Comité permanent de la Chambre des communes sur la sécurité publique et nationale, p. 22.

## LE CONTEXTE D'EXAMEN

### Recommandations du Sous-comité de la Chambre des communes et du Comité sénatorial spécial sur la Loi antiterroriste

Durant l'année écoulée, j'ai pu formuler certaines critiques à l'endroit de pratiques du CSTC qui, à mon avis, auraient avantage à être renforcées. J'estime toutefois que le fait saillant des derniers mois a été la manière dont le chef du CSTC a traité une question opérationnelle découverte à la fin de 2006 et qui posait un risque de non-conformité avec la loi. Le chef m'a informé de la situation sur-le-champ et il m'a ensuite tenu régulièrement au courant de toutes les mesures correctives prises. Par sa réaction mesurée, la direction du Centre a répondu aux besoins de l'organisation et a su montrer du respect pour les personnes qui en assurent le fonctionnement, tout en ne laissant planer aucun doute quant à leurs obligations.

Dans le rapport final qu'il a présenté à la Chambre des communes le 27 mars 2007, le Sous-comité de la Chambre des communes chargé d'examiner la *Loi antiterroriste* omnibus a formulé un certain nombre de recommandations concernant le CSTC et mon bureau, notamment sur les ambiguïtés juridiques des dispositions relatives aux autorisations ministérielles. Depuis que la *Loi antiterroriste* a reçu la sanction royale en décembre 2001, mes prédécesseurs et moi-même sommes aux prises avec un dilemme persistant qui découle des changements que cette loi a apportés à la *Loi sur la défense nationale*. Un sujet particulièrement préoccupant est la divergence de vues entre mon bureau et le CSTC concernant les avis juridiques qui lui sont prodigués par le ministère de la Justice visant l'interprétation des dispositions relatives aux autorisations ministérielles.

Dans son rapport final, le Sous-comité encourageait l'avocat du gouvernement et moi-même à régler ce différend. De plus, il demandait que, dans sa réponse au Rapport final, le gouvernement précise, dans la mesure du possible, quels étaient les points de désaccord et comment ils avaient été résolus et que, à défaut, je fournisse ces détails dans mon rapport annuel de 2007-2008.

Ce rapport annuel est le deuxième que je publie à titre de commissaire du Centre de la sécurité des télécommunications et il paraît au milieu de mon mandat de trois ans.

Une réflexion s'impose alors que j'ai franchi la moitié de mon premier mandat. Tout comme mes prédécesseurs, je veille à ce que soient respectés non seulement la lettre mais aussi l'esprit de la loi. Dans cette optique, je me penche sur des situations qui pourraient donner lieu à des activités non

conformes à la loi et je formule mes recommandations de manière à écartier cette possibilité. Si j'estime qu'une telle activité peut avoir eu lieu, je dois bien entendu en informer le ministre de la Défense nationale et le procureur général du Canada.

Ceci m'amène à réfléchir sur une de mes préoccupations personnelles — le rôle de l'individu face aux comportements qu'il convient d'adopter. Pour exercer leurs fonctions, les employés du Centre de la sécurité des télécommunications Canada (CSTC)<sup>1</sup> ne doivent pas seulement posséder des compétences techniques. Il leur faut également avoir un respect fondamental pour la primauté du droit et la démocratie, ce qui englobe une attente raisonnable en matière de protection de la vie privée de tous les Canadiens. La culture organisationnelle du CSTC doit refléter ces valeurs, et le Centre doit élaborer et mettre en œuvre des politiques et des procédures qui découlent de la loi et témoignent de ces valeurs.

Il est très clair dans mon esprit que, depuis les attentats de 2001 et les activités terroristes qui ont suivi, le niveau de risque et la perception d'une menace ont augmenté pour de nombreux Canadiens, et il est peu probable que cela diminue. Cette situation impose à des gens comme les employés du CSTC un fardeau supplémentaire, car le gouvernement s'attend à ce qu'ils dépassent les aspects purement mécaniques de la collecte du renseignement. Ils sont appelés à saisir des renseignements qui serviront de fondement à des décisions judiciaises afin de protéger les Canadiens, mais de manière à protéger la vie privée.

<sup>1</sup> L'organisme porte le nom de Centre de la sécurité des télécommunications Canada depuis le 27 septembre 2007, conformément au Programme de coordination de l'image de marque du gouvernement du Canada.

*Je veille à ce que soient respectés non seulement la lettre mais aussi l'esprit de la loi.*



Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications / 23

Annexe B : Rapports classifiés au ministre, 1996-2008 / 25

Annexe C : État des dépenses, 2007-2008 / 29

Annexe D : Historique du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) / 31

Annexe E : Rôle et mandat du Centre de la sécurité des télécommunications Canada (CSTC) / 33





Très honorable Antonio Lamer  
c.p., C.C., c.d., L.L.D., d.u.

1933-2007

*Ce rapport est dédié à la mémoire du*

L'honorable Charles D. Gonthier, C.C., c.r.  
Commissaire du Centre de la  
sécurité des télécommunications



Communications Security  
Establishment Commissionner  
The Honourable Charles D. Gonthier, C.C., Q.C.

Mai 2008

Ministre de la Défense nationale  
Édifice MGen G.R. Pearkes, 13<sup>e</sup> étage  
101, promenade Colonel-By, tour nord  
Ottawa (Ontario)  
K1A 0K2

Monsieur le ministre,

Conformément au paragraphe 273.63(3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous communiquer mon rapport annuel de 2007-2008 sur mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, monsieur le ministre, l'assurance de ma haute considération.

*Charles D. Gonthier*

Charles D. Gonthier

P.O. Box/C.P. 1984, Station "B"/Succursale « B »  
Ottawa, Canada  
K1P 5R5  
(613) 992-3044 Téléc. : (613) 992-4096

Photos de la couverture : Malak

N° de cat. D95-2008

ISBN 978-0-662-05700-0

Services gouvernementaux Canada 2008

© Ministère des Travaux publics et des

Site Web : [www.ocsec-bccst.gc.ca](http://www.ocsec-bccst.gc.ca)

Téléc. : (613) 992-4096

Tél. : (613) 992-3044

K1P 5R5

Ottawa (Ontario)

C.P. 1984, Succursale « B »

de la sécurité des télécommunications

Bureau du commissaire du Centre



**Sources Mixtes**  
Groupe de produits issu de  
forêts bien gérées et d'autres  
sources contrôlées

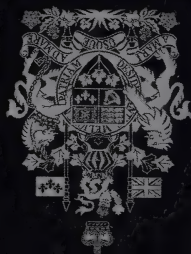
Cert no. SW-COC-000789  
[www.fsc.org](http://www.fsc.org)  
© 1996 Forest Stewardship Council

2007-2008



# Rapport annuel

COMMISSAIRE  
DU CENTRE  
DE LA SÉCURITÉ  
DES TÉLÉCOMMUNICATIONS





CA1  
ND 800  
S16



Government  
Publications

COMMUNICATIONS  
SECURITY  
ESTABLISHMENT  
COMMISSIONER

# Annual Report



2008-2009

Canada

Office of the Communications Security  
Establishment Commissioner  
P.O. Box 1984, Station "B"  
Ottawa, Ontario  
K1P 5R5

Tel.: (613) 992-3044  
Fax: (613) 992-4096  
Website: [www.ocsec-bccst.gc.ca](http://www.ocsec-bccst.gc.ca)

© Minister of Public Works and  
Government Services Canada 2009  
ISBN 978-0-662-06812-9  
Cat. No. D95-2009

Cover photos: Malak



Communications Security  
Establishment Commissioner



The Honourable Charles D. Gonthier, C.C., Q.C.

Commissaire du Centre de la  
sécurité des télécommunications

L'honorable Charles D. Gonthier, C.C., c.r.

June 2009

Minister of National Defence  
MGen G.R. Pearkes Building, 13<sup>th</sup> Floor  
101 Colonel By Drive, North Tower  
Ottawa, Ontario  
K1A 0K2



Dear Sir:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you my 2008–2009 annual report on my activities and findings, for tabling in Parliament.

Yours sincerely,

Charles D. Gonthier

P.O. Box/C.P. 1984, Station "B"/Succursale «B»  
Ottawa, Canada  
K1P 5R5  
(613) 992-3044 Fax: (613) 992-4096



---

# TABLE OF CONTENTS

Introduction /1

The Review Environment /2

- Proposed amendments to the *National Defence Act* /2
  - Ensuring the integrity of CSEC's activities and the review process /2
  - Applying a qualified opinion /3
  - Observations of the Auditor General /3
- Review cooperation /3
- Parliamentary committee involvement /4

The Year in Review /5

- Safeguarding privacy: Regular review of identity disclosures /5
- Briefings from CSEC /6
- More effective review through annual roundtables /6
- Strengthening lawful compliance /6
- A comprehensive review process /7

Methodology /8

- Identifying risks to lawfulness and privacy /8
- Attributes of a good review /8
  - Developing review findings and recommendations /9

2008–2009 Review Highlights /10

- Reviews of foreign intelligence activities under ministerial authorizations — Common elements /10
- Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) /11
- Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) /12
- Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) /14
- Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians /15
- Review of disclosure of information about Canadians to Government of Canada clients /17



- Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive /18
- Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate /19

Reviews Underway and Planned /20

Complaints about CSEC's Activities /21

Duties under the *Security of Information Act* /22

The Commissioner's Office /22

- My office's new status /22
- Canadian Association of Security and Intelligence Studies 2008 Conference /23
- International Intelligence Review Agencies Conference /23
- British Intelligence and Security Committee of Parliamentarians /24

In Closing /24

Annex A: Mandate of the Communications Security Establishment Commissioner /25

Annex B: Classified Reports, 1996–2009 /27

Annex C: Statement of Expenditures, 2008–2009 /31

Annex D: History of the Office of the Communications Security Establishment Commissioner (OCSEC) /33

Annex E: Role and mandate of the Communications Security Establishment Canada (CSEC) /35

Annex F: OCSEC Review Program — Logic Model /37

---

# INTRODUCTION

This is my third report as Communications Security Establishment Commissioner. It is an appropriate time, in my view, to reflect upon the nature of the work in which my office is engaged and the quality of the relationship that has evolved between the Communications Security Establishment Canada (CSEC) and my office.

Decades of legal experience have taught me that the most important element in any relationship is trust. This is true of all relationships, including the one between my office and CSEC. Trust, in my opinion, is not an entitlement. It is something that must be earned through integrity and professionalism. In the case of CSEC, it is also earned by demonstrating commitment to the protection of national security in a way that ensures compliance with the law and respect for the privacy of Canadians. In the case of my office, trust is earned through a rigorous, comprehensive and fair review process.

Due to the nature of its work, CSEC is required to operate largely in secrecy. The role of my office is, in part, to represent the public interest in accountability in a way that optimizes effective review while not restricting unnecessarily CSEC's legislated role.

My predecessors and I have consistently recognized prevention as an important aspect of the Commissioner's legislated role. As such, most recommendations address shortcomings in CSEC's policies, procedures and practices in order to strengthen the compliance framework and reduce any risk to privacy.

While I have, over the past three years, reported that I have found no instances of lack of compliance with the law, there may be, and have been, instances where disagreements with CSEC arise over a particular issue or where I am not satisfied with CSEC's explanation or information. In such cases, I direct my staff to pursue the issue as thoroughly as required. The manner in which such matters are handled can enhance professional trust between organizations.

As my first term draws to a close, I take satisfaction in noting that mutual trust and commitment to shared democratic values have fostered a productive working relationship. I acknowledge the leadership of CSEC which has demonstrated its commitment to lawfulness and protecting privacy.

## THE REVIEW ENVIRONMENT

### Proposed amendments to the *National Defence Act*

#### Ensuring the integrity of CSEC's activities and the review process

In last year's report I once again repeated my concern over ambiguities in Part V.I of the *National Defence Act* (NDA) with regard to CSEC's foreign intelligence activities under ministerial authorization. I recommended a number of amendments, including one to clarify the term *activity or class of activities*. I also recommended that a definition of the terms *intercept* and *interception* be inserted into the Act. I have shared with government officials these and other proposals for amendments to the NDA that I believe worthwhile to enact.

#### Ministerial authorizations — Did you know?

A ministerial authorization is a written authorization provided by the Minister of National Defence which sets out conditions CSEC must meet so as not to be in contravention of the *Criminal Code* if, in the process of conducting its foreign intelligence collection or information technology security activities, it incidentally intercepts private communications of Canadians. Ministerial authorizations may be approved or renewed for a period not exceeding one year.

---

## Applying a qualified opinion

At the end of the 2008–2009 reporting period, I continue to apply the *interim* solution put in place by my predecessors: that is, to review CSEC’s foreign intelligence collection activities under ministerial authorizations on the basis of the *NDA* as it is interpreted by Justice Canada. However, in some important respects, I disagree with that interpretation — as have both my predecessors.

In April 2006, my immediate predecessor noted in his last report as CSE Commissioner that “my one regret will be if I leave this position without a resolution of the legal interpretation issues that have bedevilled this office since December 2001.” In my 2007–2008 report, I noted the Government had indicated that legislative amendments would be brought forward “in due course”. This has yet to occur. I want to emphasize, however, that the length of time that has passed without producing amended legislation puts at risk the integrity of the review process.

## Observations of the Auditor General

I am pleased to see that the Auditor General has commented on this important matter. In a report released on March 31, 2009, she recognized that the implications of the CSE Commissioner’s qualified opinion of CSEC’s lawfulness, due to ambiguities in CSEC’s legislation, “are serious” (Section 1.14 of the *2009 Status Report of the Auditor General of Canada*).

## Review cooperation

One issue that remained unresolved in 2008–2009, stemming from Justice Dennis O’Connor’s report concerning a new review mechanism for the Royal Canadian Mounted Police’s (RCMP) national security activities, is whether there is a need for integrated review of integrated operations among enforcement and intelligence agencies. Justice O’Connor’s recommendations included “statutory gateways” to support integrated review. While cooperation among review bodies must be conducted in a manner that respects security requirements, including the *Security of Information Act*, I find no obstacles, legal or otherwise, to



---

such cooperation, if required. Moreover, I can, and do, review CSEC activities conducted under part (c) of its mandate — which involve requests for assistance to CSEC from the Canadian Security Intelligence Service (CSIS) and the RCMP — to ensure these activities are in compliance with the law.

The O'Connor inquiry included the examination of information sharing between agencies from different countries. This theme has been discussed by Canadian and international scholars. At the annual conference of the Canadian Association of Security and Intelligence Studies (CASIS), held in October 2008, reference was made to an “accountability gap”, concerning an absence of cooperation between review bodies of different countries to review information sharing agreements among their respective intelligence agencies. This is a sensitive area but one that is of great interest to me, particularly as it relates to the potential sharing of personal information about Canadians. Within my own jurisdiction, in the coming year, I will be conducting a review of CSEC's activities in this area.

## **Parliamentary committee involvement**

The Government of Canada has called for increased parliamentary involvement in the review of security and intelligence activities. Traditionally, a role for parliamentarians has been clearly established through the mechanism of Parliamentary committees: in the case of my office, it is the Standing Committee on National Defence, to which my public annual report is referred. Since the creation of the CSE Commissioner's office in 1996, the Commissioner has been invited to appear before this committee to discuss his activities and findings and to answer parliamentarians' questions quite infrequently.



---

## THE YEAR IN REVIEW

### Safeguarding privacy: Regular review of identity disclosures

Following my in-depth review of CSEC's disclosure of information about Canadians to Government of Canada clients, completed in December 2008, it was suggested by CSEC that reviews of this kind could be conducted on a regular basis. Since this CSEC activity lies at the heart of my mandate, I believe it is worthwhile to examine it regularly. As a result, my office has arranged with CSEC to begin reviews at regular intervals throughout the coming reporting year.

I believe the nature of this CSEC suggestion, and the manner in which it was presented to my office, speaks to the professional trust that has evolved in the relationship between our respective organizations. It is a positive sign, and one which I am pleased to highlight in this report.

#### **Information about Canadians — Did you know?**

When collecting foreign intelligence, CSEC may incidentally acquire information about Canadians. This information may be retained if it is assessed as essential to the understanding of the foreign intelligence. Information about Canadians may be included in foreign intelligence reporting only if it is suppressed (i.e. replaced by a generic reference such as "a Canadian person"). When receiving a subsequent request for disclosure of the details of the suppressed information, CSEC requires federal departments and agencies to explain their authority to request and use this information under their respective mandates and to provide an operational justification of their need to know this information. Only after these conditions have been met will CSEC release the suppressed information.

---

## Briefings from CSEC

My office is briefed regularly on CSEC operational policies and relevant administrative activities. In 2008–2009, my office was also provided with presentations and training in the areas of information management and information technology (IT) databases, on the safeguarding of IT networks of importance to the Government of Canada, and on the status of CSEC's policy framework. In addition, CSEC provided briefings specific to certain reviews prior to those reviews being undertaken.

## More effective review through annual roundtables

For the past two years, my staff and CSEC officials have participated in what has become an annual roundtable meeting aimed at optimizing the review process, while minimizing any adverse impact on CSEC's legislated activities. The roundtable meeting is also an opportunity to reinforce open communication and to enhance mutual understanding and trust in the working relationship between the two organizations. These meetings have proven useful in removing obstacles to effective review and will, I am sure, enable us to make progress in the years ahead.

## Strengthening lawful compliance

The objective of my review mandate is to assess whether CSEC's activities comply with the law, including the extent to which CSEC has adequate measures to protect the privacy of Canadians. While I am to report to the Minister and to the Attorney General of Canada any instances of non-compliance with the law, I also make it a point, wherever possible, to identify preventive measures that reinforce CSEC's lawful compliance.

One area in which my predecessors and I consistently called for preventive measures is improved information management practices. As we all previously noted, the absence of an adequate records management system impaired CSEC's ability to account for its activities. In response to these concerns, CSEC has taken positive steps to rectify gaps in record management practices. In fact, a new corporate records management system is expected to be fully operational during the 2009–2010 reporting period. CSEC is to be commended for its efforts in this important area.

## A comprehensive review process

In its reviews, my office sometimes goes into great depth, observing CSEC operators and analysts first hand to gain better knowledge of their work. This knowledge is particularly important when my staff examine an area in which I have made a recommendation with which CSEC disagrees.

This year, in one such case, which I describe in the section on Review Highlights, I revisited a recommendation relating to privacy, which was made last year. Following completion of a second, focussed review, I retracted that recommendation because I was satisfied that the risk to privacy was minimal and that CSEC had appropriate safeguards in place. I believe this retraction results from a rigorous but fair review approach which, in this instance, recognized the professional manner in which these particular analysts strive to conduct their work.

### Implementing recommendations — Did you know?

Since 1997, my office has submitted 52 reports to the Minister, many of which have contained substantial recommendations. CSEC has accepted and implemented and/or is working to address over 90 percent of these recommendations, which speaks to the effectiveness of the review process.

---

## METHODOLOGY

### Identifying risks to lawfulness and privacy

A key ingredient in developing a sound review selection process is the identification of activities, practices or procedures that may pose a risk to CSEC's compliance with the law. For example, these can be potential risks identified by my staff from previous or current reviews of CSEC activities, or from briefing sessions given to my staff by CSEC. CSEC may itself also identify potential risks.

In assessing topics for possible review, I instruct my staff to consider questions such as: to what extent is CSEC exposed to risk of unlawful activity in this area, and what is the likelihood that this could occur?; and if it occurs, what is the potential adverse impact?

In addition, my staff developed more detailed criteria in 2008–2009 to help determine the priority in which the identified areas of potential risk will be reviewed. These criteria, which continue to be refined, include: significant changes to authorities; changes to technology; any area that has never been reviewed in-depth, or has not been reviewed in the past four years; a follow-up to a particular recommendation I made previously; and issues arising in the public domain.

### Attributes of a good review

In conducting a review, my staff examine all relevant written and electronic records, files, correspondence and other documentation. My staff conduct interviews with CSEC managers and staff involved in the activities being reviewed and visit CSEC facilities to conduct checks, including CSEC databases. The results of reviews are shared with CSEC and, in most instances, CSEC takes action to strengthen compliance with the law or policy.

One of my primary concerns in the review of CSEC activities is ensuring that each review is based upon appropriate evidence to support all findings, conclusions and recommendations. This means that all evidence gathered must be directly *relevant*, *replicable* and *valid*.



## Review evidence — Did you know?

Evidence is information and data that are collected and used to provide a factual basis for developing findings and recommendations against review criteria.

*Relevant*: refers to the extent to which the information bears a clear and logical relationship to the review objective(s) and criteria. If information is not relevant, it cannot be evidence. *Replicable*: concerns the likelihood of coming up with the same findings if all steps of the review were reproduced. *Valid*: refers to whether the information actually is what it purports to be in relation to the content, origin and timing. As a general principle, the quantity of evidence is sufficient when there is enough to persuade a reasonable person that the review findings and conclusions are valid and the recommendations are appropriate. In order to decide if the collective weight of the evidence is sufficient, I must consider the quality of the evidence gathered, and the cost of obtaining more evidence relative to its likely benefits.

## Developing review findings and recommendations

The comparison of evidence gathered against previously established review criteria results in the development of usable findings and recommendations. Review findings confirm whether criteria have been satisfactorily met, or disclose the level, nature and significance of deviations from them. The process of assessing the evidence gathered against criteria is focussed on questions such as: does a deficiency exist between findings and expectations and as established by the review criteria? what is the cause of the deficiency? what are its likely impacts? and can the deficiency be corrected?



---

## 2008–2009 REVIEW HIGHLIGHTS

During the 2008–2009 reporting period, my office completed seven reviews on different aspects of CSEC activities. The reviews were carried out under my authority as articulated in paragraph 273.63(2)(a) and subsection 273.65(8) of the *NDA*.

The primary objective of the reviews, consistent with my mandate, was to assess whether the activities complied with the law, including the extent to which CSEC has adequate measures in place to protect the privacy of Canadians. I am able to report that the activities examined in 2008–2009 complied with the law.

With respect to the first three of the reviews listed below, in which I have reviewed different foreign intelligence collection activities conducted under ministerial authorizations, I reiterate that, pending amendments to clarify the *NDA*, these reviews are based on legal interpretation provided to CSEC by Justice Canada.

### Reviews of foreign intelligence activities under ministerial authorizations — Common elements

Paragraph 273.64(1)(a) of the *NDA* authorizes CSEC to collect foreign intelligence in accordance with the Government of Canada’s intelligence priorities. In the case of each of the CSEC foreign intelligence collection activities reviewed by my office in 2008–2009, CSEC obtained the ministerial authorization pursuant to subsections 273.65(1) and (2) of the *NDA* because, in carrying out the activities, it was possible that CSEC might intercept communications that either originated or terminated in Canada, and which constituted “private communications”, as defined in the *Criminal Code*.

The *NDA* requires that foreign intelligence collection activities not be directed at Canadians or any person in Canada (paragraph 273.64(2)(a)), and that they be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information (paragraph 273.64(2)(b)).

---

# **Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1)**

## **Background**

This review examined certain CSEC foreign intelligence collection activities conducted under three successive ministerial authorizations in effect between 2004 and 2007. Two previous reviews of these same activities conducted by my office in 1999 and 2005 respectively were taken into consideration.

## **Findings**

Based on the information reviewed and interviews conducted, I found that CSEC's activities were authorized and carried out in accordance with the law, ministerial requirements, and its operational policies and procedures.

However, the review found that additional information should be recorded and reported to the Minister in order to enhance accountability. This additional information concerns the foreign intelligence CSEC collects under this ministerial authorization and which it shares with its principal partners outside Canada. The sharing of information about Canadians is an area that my office will continue to examine.

The review also found that a memorandum of understanding between CSEC and a federal department respecting these activities should be updated to reflect current practices. In the meantime, CSEC agreed to continue to follow the terms of the existing agreement and to document any new understandings.

In addition, my staff identified certain deficiencies in CSEC policies and procedures related to the activities reviewed.

---

## **Recommendations**

As a result of these findings, I recommended that CSEC adopt and publish additional written guidance respecting the process its analysts are to follow when making targeting decisions. I also recommended that CSEC amend its policy respecting the deletion of private communications recognized by analysts and found to have no foreign intelligence value. The *NDA* requires that an intercepted private communication shall be used or retained only if it is essential to international affairs, defence or security (paragraph 273.65(2)(d)).

I am pleased to note that CSEC accepted the recommendations, and is making improvements in areas where deficiencies were identified, including making changes to its systems.

## **Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2)**

### **Background**

This review examined certain other CSEC foreign intelligence collection activities conducted under four ministerial authorizations in effect from 2004 to 2007. The review included an examination of CSEC's reporting of the foreign intelligence to its partners in Canada and abroad.

### **Findings**

Based on the information reviewed and interviews conducted, I found that the activities were authorized and complied with the law and with CSEC operational policies and procedures. Personnel responsible for the collection and management of intelligence activities were interviewed and found to be knowledgeable about the legislative authorities, policies and procedures that govern CSEC's collection.

---

However, the review also found that CSEC did not meet two of the expectations set out in the ministerial authorizations. In one instance, it was noted that CSEC did not meet a requirement to report in a timely manner to the Minister of National Defence following the expiration of the ministerial authorization. My staff found that the report was not received by the Minister's office until almost one year later.

Secondly, it was noted that in one instance CSEC did not report to the Minister an important increase in the number of private communications it inadvertently intercepted. CSEC subsequently provided my office with an explanation for this omission. Nevertheless, in reviewing this issue, I assessed that the information should have been reported in order to meet the ministerial expectation.

My report to the Minister of National Defence also suggested that CSEC introduce a greater degree of rigour in methodology applied to assessing the value of foreign intelligence reporting.

### **Recommendation**

In addressing the expectation regarding private communications, I recommended that CSEC make an explicit statement to address each ministerial expectation separately in future reports to the Minister. I am pleased to note that CSEC accepted this recommendation.

---

## **Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3)**

### **Background**

This review examined a third type of CSEC foreign intelligence collection activity conducted under three successive ministerial authorizations in effect from 2004 to 2007. In addition, the review examined CSEC's compliance with the expectations set out in a related ministerial directive, issued pursuant to subsection 273.62(3) of the *NDA*.

### **Findings**

Based on the information reviewed and interviews conducted, I found that CSEC's activities were authorized and complied with the law. I did, however, set out specific findings and made recommendations that I believe would strengthen CSEC's practices and compliance with its policies and procedures.

The review also found that CSEC did not meet one expectation set out in the ministerial directive. However, practices at the working level resulted in the fulfilment of the intention of that expectation.

Rigorous business practices at the working level throughout the development, approval and execution of these activities give a high level of assurance that the activities are conducted as approved. The review did not find the same level of clarity, rigour and record keeping in some parts of the program management processes. As a consequence, I made three recommendations.



---

## Recommendations

With respect to CSEC not meeting one expectation of the ministerial directive, and to ensure continuity of practice through time and any staff turnover, I recommended that CSEC include certain measures in its policies or procedures.

Second, while CSEC personnel demonstrated a clear understanding of associated policies and procedures, and there was no suggestion of non-compliance, I recommended that written guidelines be put in place to address certain deficiencies in policies and procedures.

Finally, the record of specific activities is comprehensively documented. In contrast, however, the record of decision related to the management of the program is incomplete. I recommended that both components be subject to the proper application of sound records management processes. As I observed previously, CSEC has been implementing a new records management system and is keeping my office informed of progress, which I am following with interest. I am pleased to note that CSEC has accepted these recommendations and is taking measures to address each of them.

## Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians

### Background

My office reviewed CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians, in accordance with subsection 273.64(2) of the *NDA*.

---

Two types of technologies were studied in this review: a foreign intelligence acquisition system and an analytical tool. The foreign intelligence acquisition system is used to acquire, process and collect information from the global information infrastructure. The analytical tool is used to support CSEC's collection of foreign intelligence and to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada (IT security). My staff observed demonstrations of the two technologies and queried CSEC operators on various aspects of their use.

## **Findings**

Based on the information reviewed and interviews conducted, I found that CSEC's activities were carried out in accordance with the law. CSEC uses these two technologies to fulfill its legislated mandate and demonstrated that it would modify its technologies, if required, to comply with its statutory obligations to protect the privacy of Canadians. The acquisition, implementation and use of these technologies helps CSEC protect the privacy of Canadians by identifying potential private communications as well as personal information about Canadians.

The review found that special attention should be brought to the development of IT security policy instruments so as to ensure that CSEC's guidance in this regard is up-to-date and formalized at the highest level. There was a difference in practices between CSEC's two business-lines (IT security and foreign intelligence collection) with regard to accounting for personal information identified through analysis. CSEC provided a reasonable explanation for this difference.

---

## Recommendation

I made one recommendation regarding requests for foreign intelligence ministerial authorizations. Since there is a risk of intercepting private communications when using the foreign intelligence acquisition system reviewed, a ministerial authorization was required. I recommended that CSEC re-evaluate how it describes foreign intelligence activities in its requests for ministerial authorizations so as to be more precise about the activities the Minister of National Defence is authorizing. I am pleased to note that CSEC accepted the recommendation.

## Review of disclosure of information about Canadians to Government of Canada clients

### Background

As part of its mandate to provide foreign intelligence in accordance with Government of Canada intelligence priorities, CSEC disseminates classified reports to federal government departments and agencies that have demonstrated requirements for the information, based on their respective mandates. These reports are authored by CSEC as well as allied agencies and may contain suppressed information about Canadians if it is essential to the understanding of the report (see: *Information about Canadians — Did you know?*).

### Findings

Based on the information reviewed and interviews conducted, I found that CSEC's activities complied with the law and with its operational policies and procedures. I made no recommendations.

---

## **Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive**

### **Background**

Last year, I reported on certain activities undertaken by CSEC under a ministerial directive and in support of its foreign intelligence collection mandate. As indicated in my 2007–2008 Annual Report, I suggested that CSEC re-examine its practice that only those private communications recognized by certain staff be accounted for. I recommended that other staff who observe and handle private communications should also be responsible for accounting for them. CSEC did not accept this recommendation, and, as a result, I directed my staff to conduct a follow-up review of these activities.

This second, focussed review, with direction to probe this matter as deeply as necessary, aimed to acquire greater knowledge about this activity, to examine the risk to privacy, and to determine if CSEC's measures to protect the privacy of Canadians were sufficient in this instance.

The goal of this review was ultimately to determine whether my recommendation of 2007–2008 should be maintained, amended or retracted. Review methodology included first-hand observation of the activities of CSEC front-line personnel conducting this activity.

### **Findings**

The review, based on detailed knowledge and understanding of activities observed by my staff, found that CSEC conducts these activities in accordance with the law and ministerial requirements, and in accordance with operational policies and procedures.

---

Based on the current practices, as observed in detail on two separate occasions, I assessed that the activities examined in this review involve only a low risk to privacy. CSEC staff conducting the activities have a different and lesser potential of affecting the privacy of Canadians than other staff conducting different activities and who are already required to account for private communications.

In addition, I assessed that CSEC has sufficient measures in place to protect the privacy of Canadians during its conduct of these activities. Personnel were aware of and followed operational policies and procedures that provide direction with respect to the protection of the privacy of Canadians.

I am pleased to note that CSEC recently revised its operational policy on this subject to include additional guidance respecting the protection of the privacy of Canadians. Managers routinely and closely monitor compliance with applicable policies and procedures. The people with whom my staff spoke were forthcoming and demonstrated a professional approach.

Therefore, in view of these findings, I retracted my previous recommendation and informed CSEC that I have no expectation of corrective action in regard to these activities.

## **Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate**

### **Background**

The specific objective of this review was to acquire knowledge of CSEC's activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate. I examined CSEC's compliance with the expectations set out in the ministerial directive and associated policies and procedures. These expectations are administrative in nature and relate primarily to security and risk management.



---

## **Findings**

Based on the information reviewed and interviews conducted, I found that CSEC's activities were consistent with the foreign intelligence priorities of the Government of Canada, and were carried out in accordance with the law and with CSEC operational policies and procedures. CSEC had also taken specific measures to protect the privacy of Canadians. I also found that, for the most part, CSEC conducted the activities in accordance with expectations set out in the ministerial directive and with associated policies and procedures.

## **Recommendations**

I recommended, however, that CSEC reconcile certain discrepancies between ministerial expectations and its own practices. I also recommended that CSEC review, update and finalize certain key documents respecting these activities, and that it clarify certain terms used in the documents. I believe this will strengthen CSEC's ability to meet the ministerial expectations and therefore enhance accountability. I am awaiting CSEC's response to these recommendations.

## **REVIEWS UNDERWAY AND PLANNED**

I am pleased to note that of the reviews I indicated were underway in my report last year, all were completed, though the results of the comprehensive study of CSEC's information technology security activities will be submitted to the Minister early in the next reporting year. In addition, the examination of certain common practices of CSEC related to its mandated activities, has been split into several reviews to permit more detailed examination. The first of these, on disclosure of information about Canadians, was completed and submitted to the Minister in this reporting year.

---

Other reviews that are underway or planned for the next reporting year include: CSEC’s foreign intelligence sharing with international partners; activities conducted under foreign intelligence ministerial authorizations; activities conducted under IT security ministerial authorizations; the process by which CSEC determines that targets of foreign intelligence interest are indeed foreign entities located outside Canada, as required by law; and CSEC’s assistance (under part (c) of its mandate) to the Canadian Security Intelligence Service under section 16 of the *CSIS Act*.

Some of these reviews may carry over into the 2010–2011 reporting year. There may also be a certain area or activity that, as a result of various factors, I determine to be a priority, resulting in it being reviewed sooner rather than later. This situation is part of the ongoing process of assessing where risks to lawful compliance or privacy are greatest.

## COMPLAINTS ABOUT CSEC’S ACTIVITIES

My mandate includes undertaking any investigation I deem necessary in response to a complaint in order to determine whether CSEC engaged, or is engaging, in unlawful activity.

This year my office received one complaint warranting investigation. While I cannot speak to the substance of the complaint, I am able to report that the investigation found no unlawful activity on the part of CSEC.

---

## DUTIES UNDER THE *SECURITY OF INFORMATION ACT*

I have a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy and seek to defend the release of classified information about CSEC on the grounds that it is in the public interest. No such matters were reported to my office in the 2008–2009 reporting period.

## THE COMMISSIONER'S OFFICE

During 2008–2009, I met periodically with the Chief of CSEC to discuss issues of mutual interest. These collaborative meetings reflect a productive working relationship which, I believe, contributes to the overall efficiency and effectiveness of the review process.

I had occasion during the reporting period to meet the Prime Minister's newly appointed National Security Advisor, whose duties include accountability for CSEC policy and operational direction. I also met with several federal court judges and other senior government officials.

## My office's new status

As I observed in my last report, a decision was taken in the autumn of 2007 that would sever my office's long-standing relationship with the Privy Council Office for the provision of administrative and other support activities and transfer these responsibilities to the Department of National Defence.

---

Subsequently, it was determined that positioning my office within the same portfolio as CSEC did not have the appearance of propriety and autonomy that ought to exist between an agency and its review body. As a result, and effective April 1, 2009, my office was granted its own parliamentary appropriation. While the reporting relationship to the Minister of National Defence remains intact, as set out in the *NDA*, my office is separate from, and is not part of, that department.

These changes have, by necessity, given rise to additional expenditures for support services, with a corresponding increase in the budget which appears at Annex C. Still, I view this new status as another indication of the maturation of my office and further reinforcement of its independence.

## **Canadian Association of Security and Intelligence Studies 2008 Conference**

My office's participation in the annual CASIS conference in October 2008 afforded an excellent opportunity to exchange perspectives on security and intelligence issues, including review, with leading experts, scholars, policy makers and practitioners from across the country. My office was also pleased to mentor two Canadian graduate students in security and intelligence studies in conference events and discussions.

## **International Intelligence Review Agencies Conference**

I attended the International Intelligence Review Agencies Conference in Auckland, New Zealand in October 2008 to make a presentation to a conference panel on developing trust between a review body and the agency being reviewed, while retaining independence. In my remarks, I emphasized that building and maintaining CSEC's trust in my office, while safeguarding my office's independence, requires constant management and accommodation of interests at all levels.

---

I also emphasized that CSEC's trust in the Commissioner's office depends significantly on the demonstrable quality of its review work. As a result, my office has placed considerable emphasis on developing, documenting and implementing sound methodologies, based on accepted standards of review and informed by years of practical experience. I added that my office has developed operational policies and procedures that, among other things, provide guidance to staff in carrying out reviews, ensure a large measure of transparency and consistency in my office's work when seen from CSEC's perspective, and provide a basis for assessing and improving CSEC's own performance in implementing its mandate.

## **British Intelligence and Security Committee of Parliamentarians**

I met with the British Intelligence and Security Committee of Parliamentarians during the Committee's visit to Ottawa in March 2009. Committee members and my staff and I participated in a useful exchange of information and opinions on security and intelligence review issues of mutual interest and concern.

## **IN CLOSING**

As I conclude my first term as CSE Commissioner and prepare to embark upon a second term in August 2009 for one year, I do so with satisfaction in current achievements and a sense of optimism going forward. Over the past three years I am pleased to have established a productive working relationship with the Chief of CSEC. I look forward to building on this relationship as I continue to review CSEC's activities in accordance with my mandate. For me, comprehensive review of these activities remains both a challenging and rewarding task, and one which I am greatly honoured to carry out on behalf of Canadians.



## ANNEX A: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

### *National Defence Act – Part V.1*

- 273.63** (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.
- (2) The duties of the Commissioner are
- (a) to review the activities of the Establishment to ensure that they are in compliance with the law;
  - (b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and
  - (c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.
- (3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.
- (4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.
- (5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

- 
- (6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.
- (7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

- 273.65** (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

### *Security of Information Act*

- 15.** (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]
- (5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]
- (b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]
- (ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.

---

## ANNEX B: CLASSIFIED REPORTS, 1996–2009

1. Principal vs. agent status – March 3, 1997 (TOP SECRET)
2. Operational policies with lawfulness implications – February 6, 1998 (SECRET)
3. CSE's activities under \*\*\* – March 5, 1998 (TOP SECRET Codeword/CEO)
4. Internal investigations and complaints – March 10, 1998 (SECRET)
5. CSE's activities under \*\*\* – December 10, 1998 (TOP SECRET/CEO)
6. On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)
7. How we test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)
8. A study of the \*\*\* collection program – November 19, 1999 (TOP SECRET Codeword/CEO)
9. On \*\*\* – December 8, 1999 (TOP SECRET/COMINT)
10. A study of CSE's \*\*\* reporting process — an overview (Phase I) – December 8, 1999 (SECRET/CEO)
11. A study of selection and \*\*\* — an overview – May 10, 2000 (TOP SECRET/CEO)
12. CSE's operational support activities under \*\*\* — follow-up – May 10, 2000 (TOP SECRET/CEO)
13. Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)
14. On findings of an external review of CSE's ITS program – June 15, 2000 (SECRET)
15. CSE's policy system review – September 13, 2000 (TOP SECRET/CEO)

16. A study of the \*\*\* reporting process — \*\*\* (Phase II) – April 6, 2001 (SECRET/CEO)
17. A study of the \*\*\* reporting process — \*\*\* (Phase III) – April 6, 2001 (SECRET/CEO)
18. CSE's participation \*\*\* – August 20, 2001 (TOP SECRET/CEO)
19. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – August 20, 2001 (TOP SECRET/CEO)
20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – August 21, 2002 (SECRET)
21. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – November 13, 2002 (TOP SECRET/CEO)
22. CSE's \*\*\* activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)
23. Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)
24. CSE's activities pursuant to \*\*\* Ministerial authorizations including \*\*\* – May 20, 2003 (SECRET)
25. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part I – November 6, 2003 (TOP SECRET/COMINT/CEO)
26. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part II – March 15, 2004 (TOP SECRET/COMINT/CEO)
27. A review of CSE's activities conducted under \*\*\* Ministerial authorization – March 19, 2004 (SECRET/CEO)
28. Internal investigations and complaints — follow-up – March 25, 2004 (TOP SECRET/CEO)

29. A review of CSE's activities conducted under 2002 \*\*\* Ministerial authorization – April 19, 2004 (SECRET/CEO)
30. Review of CSE \*\*\* operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)
31. CSE's support to \*\*\* – January 7, 2005 (TOP SECRET/COMINT/CEO)
32. External review of CSE's \*\*\* activities conducted under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)
33. A study of the \*\*\* collection program – March 15, 2005 (TOP SECRET/COMINT/CEO)
34. Report on the activities of CSE's \*\*\* – June 22, 2005 (TOP SECRET)
35. Interim report on CSE's \*\*\* operations conducted under Ministerial authorization – March 2, 2006 (TOP SECRET/COMINT)
36. External review of CSE \*\*\* activities conducted under Ministerial authorization – March 29, 2006 (TOP SECRET/CEO)
37. Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – June 16, 2006 (TOP SECRET/COMINT/CEO)
38. Review of information technology security activities at a government department under ministerial authorization – December 18, 2006 (TOP SECRET)
39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – February 20, 2007 (TOP SECRET/COMINT/CEO)
40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – March 31, 2007 (TOP SECRET/COMINT/CEO)
41. Review of information technology security activities at a government department under ministerial authorization – July 20, 2007 (TOP SECRET)



42. Review of CSEC's counter-terrorism activities – October 16, 2007 (TOP SECRET/COMINT/CEO)
43. Review of CSE's activities carried out under a ministerial directive – January 9, 2008 (TOP SECRET/COMINT/CEO)
44. Review of CSEC's support to CSIS – January 16, 2008 (TOP SECRET/COMINT/CEO)
45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – March 28, 2008 (TOP SECRET/COMINT/CEO)
46. Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians – June 11, 2008 (TOP SECRET/COMINT/CEO)
47. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) – June 11, 2008 (TOP SECRET/COMINT/CEO)
48. Review of disclosure of information about Canadians to Government of Canada clients – November 19, 2008 (TOP SECRET/COMINT/CEO)
49. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) – January 13, 2009 (TOP SECRET/COMINT/CEO)
50. Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) – February 26, 2009 (TOP SECRET/COMINT/CEO)
51. Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate – March 12, 2009 (TOP SECRET/COMINT Codeword/CEO)
52. Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive – March 12, 2009 (TOP SECRET/COMINT/CEO)

---

# ANNEX C: STATEMENT OF EXPENDITURES 2008–2009

## Standard Object Summary

Salaries and Wages	\$782,686
Transportation and Telecommunications	43,337
Information	16,303
Professional and Special Services	258,294
Rentals	157,371
Purchased Repair and Maintenance	1,913
Materials and Supplies	7,822
Acquisition of Machinery and Equipment	23,595
Other Expenditures	0
<b>Total</b>	<b>\$1,291,321</b>



---

## ANNEX D: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER (OCSEC)

The Office of the Communications Security Establishment Commissioner (OCSEC) was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Québec, who held the position until June 2003. He was succeeded by the late Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., former Chief Justice of Canada for a term of three years. The Honourable Charles D. Gonthier, C.C., Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act*. During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment Canada (CSEC) to determine whether they conformed with the laws of Canada; and to receive complaints about CSEC's activities.

Following the terrorist attacks in the United States on September 11, 2001, Parliament adopted the omnibus *Anti-terrorism Act* which came into force on December 24, 2001. The omnibus *Act* introduced amendments to the *National Defence Act*, by adding Part V.1 and creating legislative frameworks for both OCSEC and CSEC. It also gave the Commissioner new responsibilities to review activities carried out by CSEC under a ministerial authorization.

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act*. This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSEC on the grounds that it is in the public interest. The legislation also continued the Commissioner's powers under the *Inquiries Act*.

---

In autumn 2007, a decision was taken that would sever OCSEC's long-standing arrangements with the Privy Council Office for administrative and other support activities. Effective April 1, 2009, OCSEC was granted its own parliamentary appropriation. While the Commissioner continues to provide the Minister of National Defence with his reports, OCSEC is separate from, and not part of, the department.



---

## ANNEX E: ROLE AND MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

The Communications Security Establishment Canada (CSEC) is Canada's national cryptologic agency. Unique within Canada's security and intelligence community, CSEC employs code-makers and code-breakers to provide the Government of Canada with information technology security and foreign intelligence services. CSEC also provides technical and operational assistance to federal law enforcement and security agencies.

CSEC's foreign intelligence products and services support government decision-making in the fields of national security, national defence and foreign policy. CSEC's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSEC's information technology security products and services enable its clients (government departments and agencies) to effectively secure their electronic information systems and networks. CSEC also conducts research and development on behalf of the Government of Canada in fields related to communications security.

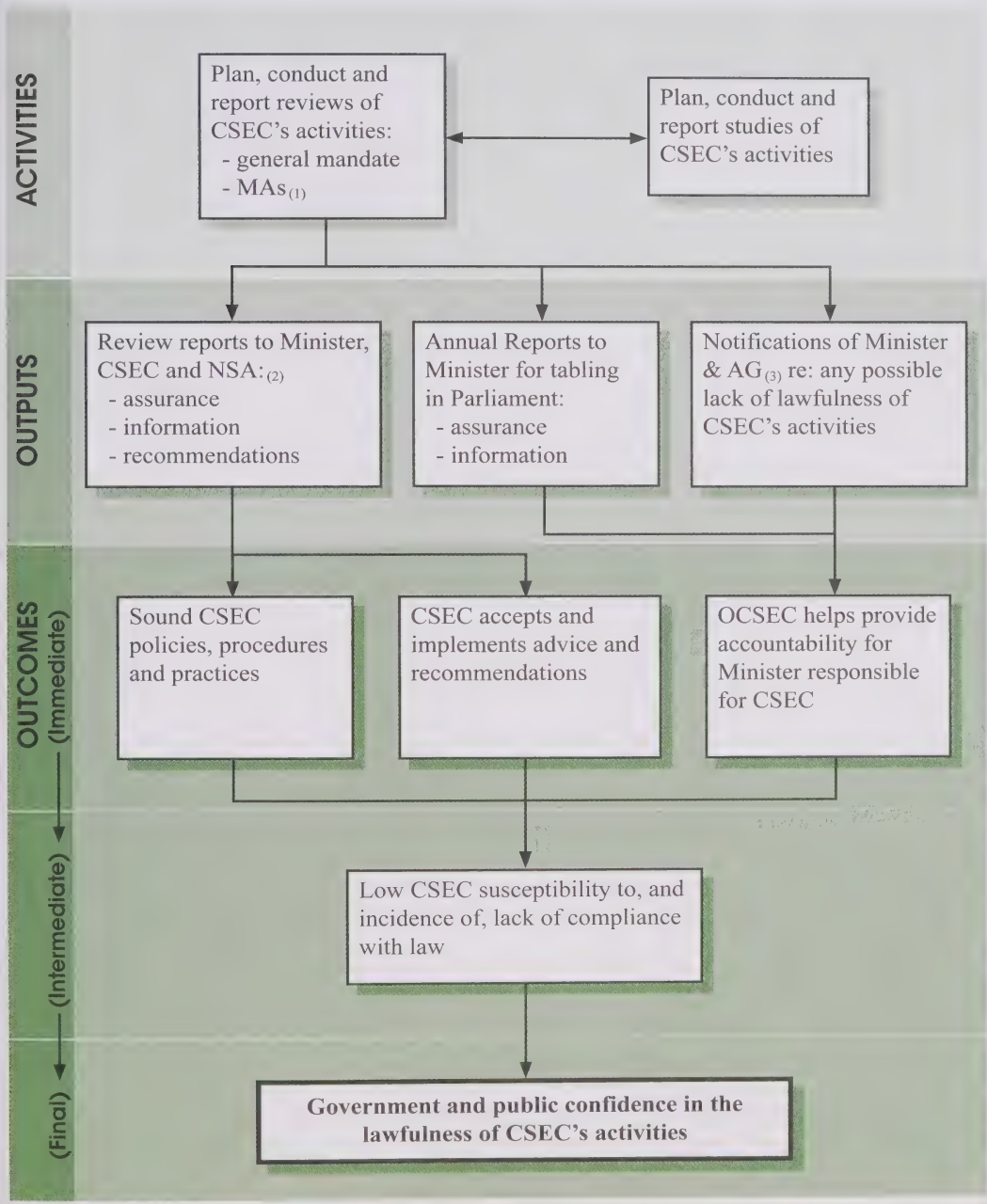
CSEC has a three-part mandate under subsection 273.64(1) of the *National Defence Act*. These are known as parts (a), (b) and (c) of its mandate:

- (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
- (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
- (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.



# ANNEX F: OCSEC REVIEW PROGRAM — LOGIC MODEL

The following logic model provides a graphic description of how the review program functions.



(1) Ministerial authorizations

(2) National Security Advisor to the Prime Minister

(3) Attorney General of Canada

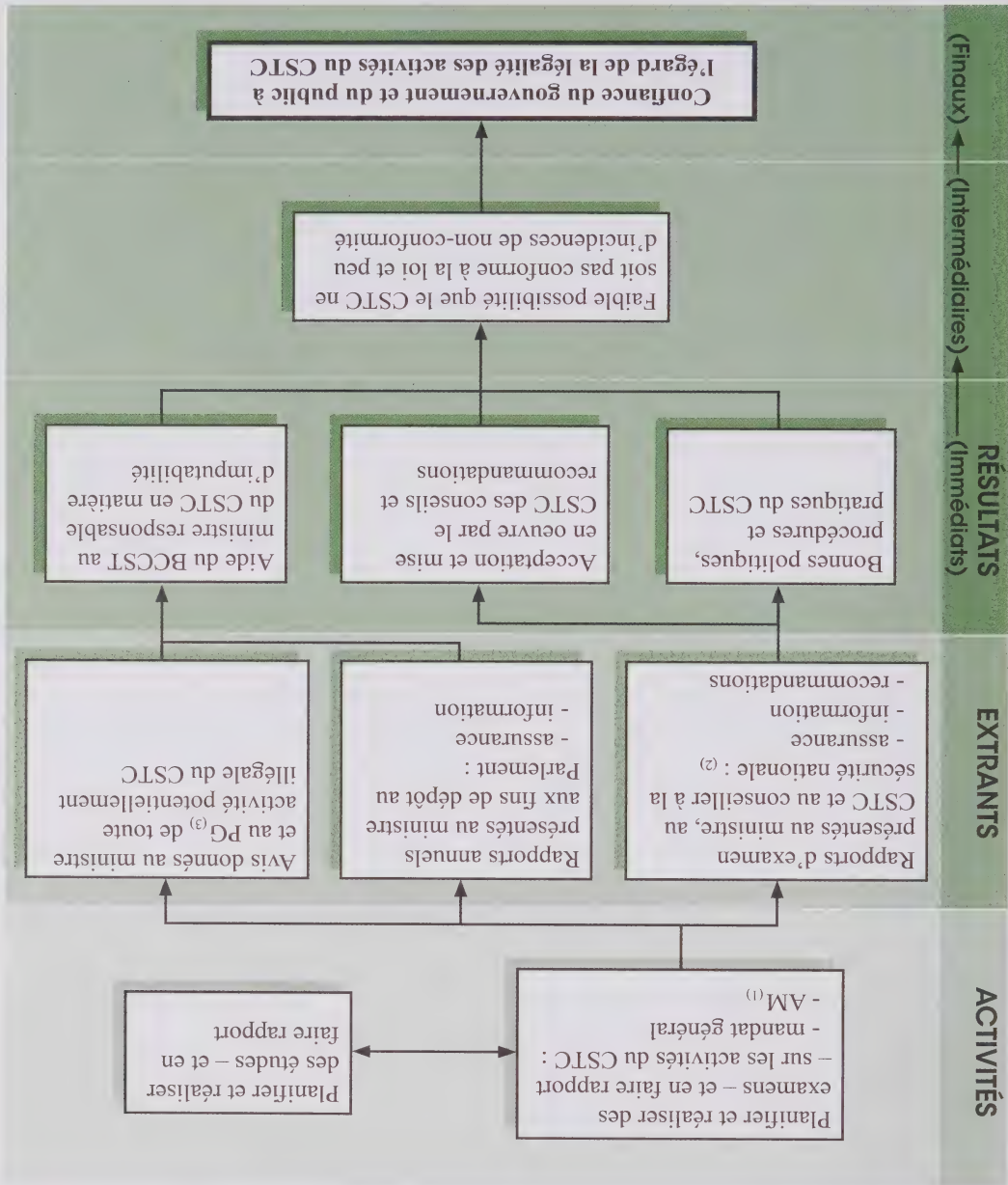






# ANNEXE F : PROGRAMME D'EXAMEN DU BCCST — MODÈLE LOGIQUE

Le modèle logique suivant offre une description graphique de la façon dont le programme d'examen fonctionne.





# ANNEXE E : RÔLE ET MANDAT DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS CANADA (CSTC)

Le Centre de la sécurité des télécommunications Canada (CSTC) est l'organisme national de cryptologie du Canada. Organisme unique en son genre au sein de la collectivité canadienne de la sécurité et du renseignement, le CSTC emploie des cryptologues pour protéger la sécurité des technologies de l'information du gouvernement du Canada et lui fournir des renseignements étrangers. Il offre en outre une assistance technique et opérationnelle aux organismes fédéraux chargés de la sécurité et de l'application de la loi. Les produits et services de renseignement étranger du CSTC sont fournis à l'appui des décisions gouvernementales dans les domaines de la sécurité nationale, du renseignement national et de la politique étrangère. Ses activités en matière de renseignement électromagnétiques visent exclusivement des renseignements étrangers et sont assujetties aux priorités du gouvernement du Canada en matière de renseignement.

Dans le domaine de la sécurité des technologies de l'information, les produits et services du CSTC permettent à ses clients (les autres ministères et organismes gouvernementaux) d'assurer la sécurité de leurs systèmes et réseaux d'information électronique. Le CSTC effectue aussi des travaux de recherche-développement au nom du gouvernement du Canada dans des disciplines liées à la sécurité des télécommunications.

Le paragraphe 273.64(1) de la partie V.1 de la *Loi sur la défense nationale* établit le mandat du CSTC, qui comprend trois volets désignés sous le nom de parties a), b) et c) :

- a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
- b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;
- c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.



## ANNEXE D : HISTORIQUE DU BUREAU DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS (BCCST)

Le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) a été créé le 19 juin 1996, au moment de la nomination du premier commissaire, l'honorable Claude Bisson, O.C., ancien juge en chef du Québec. M. Bisson a occupé le poste de commissaire jusqu'en juin 2003. Le très honorable Antonio Lamer, c.p., C.C., c.d., L.L.D., d.u., ancien juge en chef du Canada (décédé), lui a alors succédé pour un mandat de trois ans. L'honorable Charles D. Gonthier, C.C., c.r., qui a pris sa retraite de la Cour suprême du Canada en 2003, a été nommé commissaire en août 2006.

Pendant les six premières années de son mandat (de juin 1996 à décembre 2001), le commissaire a exercé ses fonctions conformément à plusieurs décrets, pris en vertu de la partie II de la *Loi sur les enquêtes*. Au cours de cette période, il a assumé une double responsabilité : examiner les activités du Centre de la sécurité des télécommunications Canada (CSTC) afin de déterminer si elles étaient en conformité avec les lois du Canada, et recevoir les plaintes relatives aux activités du CSTC.

Dans le sillage des attentats terroristes du 11 septembre 2001, le Parlement a adopté la *Loi antiterroriste* omnibus, qui a été promulguée le 24 décembre 2001. Cette *Loi* modifie la *Loi sur la défense nationale*, en y ajoutant la partie V.1, qui établit le cadre législatif du BCCST et du CSTC, et elle confie au commissaire de nouvelles responsabilités relatives à l'examen des activités que mène le CSTC sous le régime d'une autorisation ministérielle.

En outre, la *Loi* omnibus a remplacé la *Loi sur les secrets officiels* par la *Loi sur la protection de l'information*, laquelle attribue au commissaire des fonctions précises pour les cas où une personne astreinte au secret à perpétuité souhaiterait invoquer la défense de l'intérêt public pour justifier la divulgation de renseignements classifiés sur le CSTC. Il a été décidé à l'automne 2007 de mettre fin à la relation de longue date que le BCCST entretenait avec le Bureau du Conseil privé pour les fonctions de soutien administratif et autres du bureau. Le BCCST a reçu son propre crédit parlementaire le 1<sup>er</sup> avril 2009. Bien que le commissaire transmette toujours ses rapports au ministre de la Défense nationale, le BCCST est un organisme distinct, ne faisant pas partie de ce ministère.





ANNEXE C : ÉTAT DES DÉPENSES, 2008-2009

Sommaire des articles courants

Traitements et salaires	782 686 \$
Transports et télécommunications	43 337
Information	16 303
Services professionnels et spéciaux	258 294
Location	157 371
Achat de services de réparation et d'entretien	1 913
Fournitures et approvisionnements	7 822
Acquisition de machine et de matériel	23 595
Autres charges	0
Total	1 291 321 \$

42. Review of CSEC's counter-terrorism activities – 16 octobre 2007 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
43. Review of CSE's activities carried out under a ministerial directive – 9 janvier 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
44. Review of CSEC's support to CSIS – 16 janvier 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – 28 mars 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
46. Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians – 11 juin 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
47. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) – 11 juin 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
48. Review of disclosure of information about Canadians to Government of Canada clients – 19 novembre 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
49. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) – 13 janvier 2009 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
50. Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) – 26 février 2009 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
51. Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate – 12 mars 2009 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
52. Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive – 12 mars 2009 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

29. A review of CSE's activities conducted under 2002 \*\*\* Ministerial authorization – 19 avril 2004 (SECRET/Réserve aux Canadiens)

30. Review of CSE \*\*\* operations under Ministerial authorization – 1er juin 2004 (TRÈS SECRET/COMINT)

31. CSE's support to \*\*\* – 7 janvier 2005 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

32. External review of CSE's \*\*\* activities conducted under Ministerial authorization – 28 février 2005 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

33. A study of the \*\*\* collection program – 15 mars 2005 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

34. Report on the activities of CSE's \*\*\* – 22 juin 2005 (TRÈS SECRET)

35. Interim report on CSE's \*\*\* operations conducted under Ministerial authorization – 2 mars 2006 (TRÈS SECRET/COMINT)

36. External review of CSE \*\*\* activities conducted under Ministerial authorization – 29 mars 2006 (TRÈS SECRET/Réserve aux Canadiens)

37. Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – 16 juin 2006 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

38. Review of information technology security activities at a government department under ministerial authorization – 18 décembre 2006 (TRÈS SECRET)

39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – 20 février 2007 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – 31 mars 2007 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

41. Review of information technology security activities at a government department under ministerial authorization – 20 juillet 2007 (TRÈS SECRET)

15. CSE's policy system review – 13 septembre 2000 (TRÈS SECRET/Réservé aux Canadiens)
16. A study of the \*\*\* reporting process — \*\*\* (Phase II) – 6 avril 2001 (SECRET/Réservé aux Canadiens)
17. A study of the \*\*\* reporting process — \*\*\* (Phase III) – 6 avril 2001 (SECRET/Réservé aux Canadiens)
18. CSE's participation \*\*\* – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)
19. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)
20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – 21 août 2002 (SECRET)
21. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – 13 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)
22. CSE's \*\*\* activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization – 27 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)
23. Lexicon of CSE definitions – 26 mars 2003 (TRÈS SECRET)
24. CSE's activities pursuant to \*\*\* Ministerial authorizations including \*\*\* – 20 mai 2003 (SECRET)
25. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part I – 6 novembre 2003 (TRÈS SECRET/COMINT/Réservé aux Canadiens)
26. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part II – 15 mars 2004 (TRÈS SECRET/COMINT/Réservé aux Canadiens)
27. A review of CSE's activities conducted under \*\*\* Ministerial authorization – 19 mars 2004 (SECRET/Réservé aux Canadiens)
28. Internal investigations and complaints — follow-up – 25 mars 2004 (TRÈS SECRET/Réservé aux Canadiens)



## ANNEXE B : RAPPORTS CLASSIFIÉS AU MINISTRE, 1996-2009

1. Principal vs. agent status – 3 mars 1997 (TRÈS SECRET)
2. Operational policies with lawfulness implications – 6 février 1998 (SECRET)
3. CSE's activities under \*\*\* – 5 mars 1998 (TRÈS SECRET Mot codé/Réserve aux Canadiens)
4. Internal investigations and complaints – 10 mars 1998 (SECRET)
5. CSE's activities under \*\*\* – 10 décembre 1998 (TRÈS SECRET/Réserve aux Canadiens)
6. On controlling communications security (COMSEC) material – 6 mai 1999 (TRÈS SECRET)
7. How we test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) – 14 juin 1999 (TRÈS SECRET Mot codé/Réserve aux Canadiens)
8. A study of the \*\*\* collection program – 19 novembre 1999 (TRÈS SECRET Mot codé/Réserve aux Canadiens)
9. On \*\*\* – 8 décembre 1999 (TRÈS SECRET/COMINT)
10. A study of CSE's \*\*\* reporting process — an overview (Phase I) – 8 décembre 1999 (SECRET/Réserve aux Canadiens)
11. A study of selection and \*\*\* — an overview – 10 mai 2000 (TRÈS SECRET/Réserve aux Canadiens)
12. CSE's operational support activities under \*\*\* — follow-up – 10 mai 2000 (TRÈS SECRET/Réserve aux Canadiens)
13. Internal investigations and complaints — follow-up – 10 mai 2000 (SECRET)
14. On findings of an external review of CSE's ITS program – 15 juin 2000 (SECRET)

- (7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.
- [...]
- 273.65** (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.
- Loi sur la protection de l'information*
- 15.** (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]
- (5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]
- b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession : [...]
- (ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.

# ANNEXE A : MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

## Loi sur la défense nationale – partie V.1

273.63

(1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

- a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;
- b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;
- c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

mis au point des politiques et des procédures opérationnelles qui ont notamment permis d'orienter les employés dans l'exécution des examens, de garantir dans une large mesure la transparence et la cohérence du travail de mon équipe du point de vue du CSTC, et de servir de base à l'évaluation et à l'amélioration du rendement du CSTC pour la réalisation de son mandat.

## British Intelligence and Security Committee of Parliamentarians

J'ai rencontré les membres du British Intelligence and Security Committee of Parliamentarians lors de leur visite à Ottawa en mars 2009. Les membres du comité, mon personnel et moi-même avons eu des échanges d'information et de points de vue utiles sur des questions d'intérêt et des préoccupations mutuelles touchant l'examen en matière de sécurité et de renseignements.

## MOT DE LA FIN

En raison des réalisations actuelles, c'est avec satisfaction et optimisme dans l'avenir que je termine mon premier mandat à titre de commissaire du CST et que j'entreprends un deuxième mandat d'un an en août 2009. Au cours des trois dernières années, je suis heureux d'avoir établi une relation de travail productive avec le chef du CSTC. J'espère renforcer cette relation en continuant à examiner les activités de l'organisme conformément à mon mandat. Un examen exhaustif représente pour moi à la fois un défi et une tâche enrichissante que je suis fier d'accomplir au nom des Canadiens.

Ces changements ont inévitablement donné lieu à une augmentation des dépenses relatives aux services de soutien, et à une augmentation correspondante du budget qui figure à l'annexe C. J'estime que ce nouveau statut est une autre preuve de l'évolution de mon bureau et du renforcement de son indépendance.

## Conférence 2008 de l'Association canadienne pour les études de renseignement et de sécurité

Nous avons participé à la conférence annuelle de l'ACERS en octobre 2008, qui nous a donné une excellente occasion d'échanger sur les perspectives touchant les questions relatives à la sécurité et aux renseignements, y compris l'examen, avec des spécialistes, des chercheurs, des décideurs et des intervenants importants de partout au pays. Le personnel de mon bureau a beaucoup apprécié de guider deux étudiants canadiens diplômés en sécurité et renseignements dans le cadre de la conférence et des discussions.

## Conférence internationale des organismes de surveillance du renseignement

En octobre 2008, dans le cadre de la Conférence internationale des organismes de surveillance du renseignement, à Auckland, en Nouvelle-Zélande, j'ai donné un exposé devant un groupe d'experts sur la façon d'établir un lien de confiance entre un organe d'examen et l'organisme soumis à l'examen, tout en conservant son indépendance. J'ai fait ressortir que l'établissement et le maintien du lien de confiance entre le CSTC et mon bureau, et la protection de l'indépendance de mon bureau, nécessitent une gestion constante des intérêts à tous les niveaux et des accommodements à cet égard.

J'ai également mis l'accent sur le fait que la confiance du CSTC à l'égard du Bureau du commissaire repose en grande partie sur la qualité évidente de ses examens. C'est pourquoi mon bureau attache une grande importance à l'élaboration, à la consignation et à la mise en œuvre de méthodes solides, reposant sur des normes acceptées en matière d'examen et plusieurs années d'expérience pratique. J'ai ajouté que mon bureau avait



## FONCTIONS EXERCÉES EN VERTU DE LA LOI SUR LA PROTECTION DE L'INFORMATION

### LE BUREAU DU COMMISSAIRE

Au cours de 2008–2009, j'ai rencontré périodiquement le chef du CSTC pour discuter de questions d'intérêt mutuel. Ces rencontres de collaboration témoignent d'une relation de travail productive qui, selon moi, favorise l'efficacité et l'efficience générales du processus d'examen. Au cours de la période de référence, j'ai eu l'occasion de rencontrer la conseillère à la sécurité nationale nouvellement nommée par le premier ministre, dont les responsabilités incluent celles relativement aux politiques et au fonctionnement du CSTC. J'ai également rencontré certains juges de la cour fédérale ainsi que d'autres hauts fonctionnaires.

### Nouveau statut de mon bureau

Comme je l'ai mentionné dans mon dernier rapport, il a été décidé à l'automne 2007 de mettre fin à la relation de longue date que mon bureau entretenait avec le Bureau du Conseil privé et de confier au ministre de la Défense nationale les fonctions de soutien administratif et autres de mon bureau.

Par la suite, il a été établi que le positionnement de mon bureau au sein du même portefeuille que le CSTC semblait heurter les convenances et nuire à l'autonomie qui doit exister entre un organisme et son organe d'examen. Par conséquent, à compter du 1<sup>er</sup> avril 2009, mon bureau s'est vu accorder son propre crédit parlementaire. Bien que le lien hiérarchique avec le ministre de la Défense nationale demeure inchangé, comme le prévoit la *Loi sur la défense nationale*, mon bureau est un organisme distinct ne faisant pas partie de ce ministère.

Mon mandat consiste notamment à entreprendre toute enquête que je juge nécessaire à la suite d'une plainte afin de déterminer si le CSTC a mené ou même des activités illégales.

Cette année, mon bureau a reçu une plainte justifiant la tenue d'une enquête. Bien que je ne puisse commenter la teneur de la plainte, je suis en mesure d'affirmer que l'enquête a permis de conclure que le CSTC ne s'était livré à aucune activité illégale.

## PLAINTES AU SUJET DES ACTIVITÉS DU CSTC

Voici les autres examens en cours ou projetés pour la prochaine année : l'échange des renseignements étrangers du CSTC à ses partenaires internationaux; activités menées en vertu d'autorisations ministérielles en matière de renseignements étrangers; activités menées en vertu d'autorisations ministérielles relatives à la sécurité des TI; processus permettant au CSTC d'établir que les cibles de renseignements étrangers sont bien des entités étrangères situées en dehors du Canada, comme le prescrit la Loi; assistance du CSTC au Service canadien du renseignement de sécurité (conformément à la partie c) de son mandat) en vertu de l'article 16 de la Loi sur le service canadien du renseignement de sécurité.

Certains de ces examens pourraient se poursuivre en 2010-2011. Si j'estime qu'en fonction de certains facteurs des questions ou des activités sont prioritaires, elles pourraient être examinées plus rapidement. Cette situation fait partie du processus continu d'examen visant à recenser les secteurs où les risques d'atteinte à la loi ou à la vie privée sont les plus importants.

## Conclusions

Selon les renseignements examinés et les entrevues menées, j'ai conclu que les activités étaient conformes aux priorités du gouvernement du Canada en matière de renseignements étrangers ainsi qu'à la loi et aux politiques et procédures opérationnelles de l'organisme. Le CSTC avait également pris des mesures précises pour protéger la vie privée des Canadiens. J'ai en outre conclu qu'en général le CSTC menait ses activités conformément aux attentes figurant dans la directive ministérielle et aux politiques et procédures connexes.

## Recommandations

Toutefois, j'ai recommandé au CSTC de combler certains écarts entre les attentes ministérielles et ses propres pratiques. J'ai aussi conseillé à l'organisme d'examiner, de mettre à jour et de compléter certains documents clés relatifs à ces activités et de clarifier certains termes y figurant. Je crois que cette mesure permettra au CSTC de mieux répondre aux exigences ministérielles, augmentant ainsi l'imputabilité. J'attends la réponse du CSTC à mes recommandations.

## EXAMENS EN COURS OU PROJÉTÉS

Je suis heureux de constater que les examens en cours figurant dans mon rapport de l'an dernier sont tous terminés; les résultats de l'étude exhaustive des activités du CSTC en matière de sécurité des technologies de l'information sera cependant présentée au ministre au début de la prochaine année de référence. En outre, l'examen de certaines pratiques communes du CSTC touchant les activités prescrites en vertu de son mandat a été scindé en plusieurs examens afin de permettre une étude plus approfondie. Le premier examen, qui portait sur la divulgation de renseignements au sujet de Canadiens, est terminé et a été présenté au ministre pendant la présente année de référence.

L'objectif précis de cet examen visait à connaître les activités du CSTC menées en vertu d'une autorisation ministérielle et à l'appui de son mandat en matière de collecte de renseignements étrangers. J'ai examiné la conformité du CSTC aux attentes figurant dans la directive ministérielle et aux politiques et procédures connexes. Ces attentes sont de nature administrative et touchent principalement la sécurité et la gestion du risque.

## Contexte

# Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une directive ministérielle et à l'appui de son mandat en matière de collecte de renseignements étrangers

D'après les pratiques en vigueur, telles qu'elles ont été observées en détail à deux reprises, j'estime que les activités soumises à l'examen ne présentent qu'un faible risque pour la vie privée. Les employés du CSTC qui en sont chargés ont moins de chances de porter atteinte à la vie privée des Canadiens que ceux qui effectuent d'autres activités et qui sont déjà tenus de rendre compte des communications privées.

En outre, j'estime que le CSTC a mis en place des mesures suffisantes afin de protéger la vie privée des Canadiens lorsqu'il mène ces activités. Les employés connaissent et respectaient les politiques et les procédures opérationnelles dans lesquelles figurent les directives à cet égard.

Je suis heureux de constater que le CSTC a récemment révisé sa politique opérationnelle à ce sujet pour y ajouter des directives supplémentaires en matière de protection de la vie privée des Canadiens. Les gestionnaires surveillent régulièrement et de près la conformité aux politiques et aux procédures applicables. Les personnes à qui les membres de mon équipe ont parlé se sont montrées très ouvertes et ont fait preuve de professionnalisme à l'égard des activités soumises à l'examen.

Ainsi, compte tenu de ces conclusions, j'ai rétracté ma recommandation antérieure et informé le CSTC que je ne m'attends pas à ce qu'il prenne des mesures correctives quant à ces activités.



## Suivi d'une recommandation découlant de l'examen effectué en 2007-2008 relativement à des activités du CSTC exercées en vertu d'une directive ministérielle

### Contexte

L'an dernier, j'ai présenté mes observations sur certaines activités du CSTC exercées en vertu d'une directive ministérielle et visant à appuyer son mandat en matière de collecte de renseignements étrangers. Comme je l'indiquais dans mon rapport annuel 2007-2008, j'ai recommandé au CSTC de réexaminer sa pratique selon laquelle seulement les communications privées reconnues par certains membres du personnel doivent faire l'objet d'un rapport. J'ai recommandé que d'autres employés qui observent et traitent des communications privées soient également tenus de rendre compte de ces communications. Le CSTC a rejeté cette recommandation, et j'ai donc demandé aux membres de mon équipe de mener un examen de suivi concernant ces activités.

Ce deuxième examen approfondi, assorti d'une directive permettant d'examiner la question de manière aussi approfondie que nécessaire, visait à mieux connaître cette activité, à examiner les risques pour la vie privée et à établir si les mesures prises par le CSTC pour protéger la vie privée des Canadiens étaient suffisantes.

L'examen avait pour objectif ultime de déterminer si je devais maintenir, modifier ou rétracter la recommandation que j'avais formulée en 2007-2008. La méthode d'examen comprenait l'observation directe des activités du personnel de première ligne du CSTC.

### Conclusions

L'examen, reposant sur une connaissance et une compréhension précises des activités observées par les membres de mon équipe, a révélé que le CSTC mène ces activités dans le respect de la loi et des exigences ministérielles, et conformément aux procédures opérationnelles.



J'ai formulé une recommandation au sujet des demandes d'autorisation ministérielle en matière de renseignements étrangers. Comme des communications privées peuvent être interceptées par le système d'acquisition de renseignements étrangers soumis à l'examen, une autorisation ministérielle est nécessaire. J'ai recommandé au CSTC d'examiner de nouveau la façon dont il décrit les activités en matière de renseignements étrangers dans ses demandes d'autorisation ministérielle, afin de mieux préciser les activités que le ministre de la Défense nationale autorise. Je suis heureux de constater que le CSTC a accepté cette recommandation.

## Examen de la divulgation de renseignements sur les Canadiens aux clients du gouvernement du Canada

### Contexte

Dans le cadre de son mandat visant à fournir des renseignements étrangers conformément aux priorités du gouvernement du Canada en matière de renseignements, le CSTC transmet ses propres rapports classifiés, ainsi que ceux des agences alliées, aux ministères et organismes fédéraux qui ont un besoin prouvé en matière de renseignement, en fonction de leur mandat respectif. Ces rapports sont préparés par le CSTC ainsi que par des partenaires internationaux et ils peuvent contenir des renseignements supprimés au sujet de Canadiens si cela est indispensable à la compréhension du rapport (voir l'encadré *Renseignements sur les Canadiens — Qu'en est-il?*).

### Conclusions

À la lumière des renseignements examinés et des entrevues effectuées, j'ai conclu que les activités du CSTC étaient autorisées et conformes à la loi ainsi qu'aux politiques et aux procédures opérationnelles de l'organisme. Je n'ai formulé aucune recommandation.

L'examen visait deux types de technologies : un système d'acquisition de renseignements étrangers et un outil analytique. Le premier est utilisé pour acquérir, traiter et recueillir des renseignements provenant de l'infrastructure mondiale d'information. Le second appuie la collecte de renseignements étrangers et aide l'organisme à assurer la protection des renseignements électroniques et des infrastructures d'information importantes pour la sécurité du gouvernement du Canada sur le plan des technologies de l'information (sécurité des TI). Les membres de mon équipe ont assisté à des démonstrations touchant les deux technologies et ils ont interrogé les opérateurs du CSTC au sujet de différentes facettes de leur utilisation.

**Conclusions**

D'après les renseignements examinés et les entrevues, j'ai conclu que les activités du CSTC étaient conformes à la loi. Le CSTC utilise ces deux technologies pour s'acquitter du mandat que lui confère la loi, et il a démontré qu'il modifierait ses technologies le cas échéant pour se conformer à ses obligations statutaires en matière de protection de la vie privée des Canadiens. L'acquisition, la mise en œuvre et l'utilisation de ces technologies aident l'organisme en lui permettant de détecter les communications pouvant être privées ainsi que les renseignements personnels au sujet des Canadiens.

L'examen a révélé que l'élaboration des instruments de politique relatifs à la sécurité des TI devrait faire l'objet d'une attention particulière, pour faire en sorte que les directives du CSTC dans ce domaine soient à jour et officialisées au plus haut niveau. Il existe une différence entre les pratiques relatives aux deux secteurs d'activité du CSTC – la sécurité des TI et la collecte de renseignements étrangers – en ce qui a trait à la reddition de comptes en matière de renseignements personnels détectés au moyen d'analyses. Le CSTC a fourni une explication raisonnable au sujet de cette différence.

## Recommandations

En ce qui concerne le non-respect d'une attente figurant dans la directive ministérielle et pour assurer que l'organisme maintienne ses pratiques au fil du temps et malgré le roulement de personnel, j'ai recommandé au CSTC d'ajouter certaines mesures à ses politiques ou procédures.

Deuxièmement, bien que le personnel du CSTC ait montré une bonne compréhension des politiques et procédures connexes et que rien n'indique la non-conformité, j'ai recommandé qu'on établisse des lignes directrices écrites pour combler certaines lacunes des politiques et procédures.

Enfin, le compte rendu d'activités précises est consigné en détail. Par contre, le compte rendu des décisions relatives à la gestion du programme est incomplet. J'ai recommandé qu'on applique correctement à ces deux éléments des processus valables de gestion des documents. Comme je l'ai mentionné précédemment, le CSTC est en train de mettre en œuvre un nouveau système de gestion des documents et il me tient au courant du déroulement de ce projet, que je suis avec intérêt. Je suis heureux de constater que le CSTC a accepté ces recommandations et prend des mesures pour répondre à chacune d'entre elles.

## Examen de l'acquisition et de la mise en œuvre des technologies par le CSTC comme moyen de protéger la vie privée des Canadiens

### Contexte

Mon bureau a examiné l'acquisition et la mise en œuvre par le CSTC de technologies permettant de protéger la vie privée des Canadiens conformément aux dispositions du paragraphe 273.64(2) de la LDN.

# Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une directive ministérielle et d'une autorisation ministérielle (activité 3)

## Contexte

Cet examen touchait un troisième type d'activités de collecte de renseignements étrangers menées par le CSTC en vertu de trois autorisations ministérielles successives en vigueur de 2004 à 2007. En outre, l'examen portait sur la conformité du CSTC aux attentes figurant dans une directive ministérielle connexe, émise conformément au paragraphe 273.62(3) de la LDN.

## Conclusions

En me fondant sur les renseignements examinés et sur les entrevues, j'ai conclu que les activités du CSTC étaient autorisées et conformes à la loi. Toutefois, j'ai présenté des conclusions précises et formulé des recommandations qui, selon moi, permettraient de renforcer les pratiques du CSTC et la conformité à ses politiques et procédures.

L'examen a également permis d'établir que l'organisme n'avait pas respecté une attente énoncée dans la directive ministérielle. Toutefois, les pratiques opérationnelles ont permis de satisfaire aux buts de cette attente. Des pratiques opérationnelles rigoureuses en matière d'élaboration, d'approbation et d'exécution de ces activités permettent de conclure avec un degré de confiance élevé que ces dernières sont menées conformément aux autorisations. Nous n'avons cependant pas trouvé le même niveau de clarté, de rigueur et de tenue de dossier en ce qui a trait à certaines parties des processus de gestion du programme. Par conséquent, j'ai émis trois recommandations.

d'établir que les employés chargés de la collecte des renseignements et de la gestion des activités connexes connaissent bien les autorisations législatives, les politiques et les procédures qui régissent la collecte de renseignements par le CSTC.

Toutefois, l'examen a également permis d'établir que le CSTC n'avait pas respecté deux des attentes énoncées dans les autorisations ministérielles. Dans un cas, j'ai noté que le CSTC n'avait pas respecté une exigence relative à la présentation d'un rapport en temps opportun au ministre de la Défense nationale, après l'expiration de l'autorisation ministérielle. Mon équipe a constaté que le bureau du ministre avait reçu ledit rapport près d'un an plus tard.

J'ai en outre constaté que, dans un cas, le CSTC n'avait pas informé le ministre d'une augmentation marquée du nombre de communications privées interceptées par inadvertance. Par la suite, l'organisme nous a fourni une explication à cet égard. Néanmoins, en examinant cette question, j'ai établi que ces renseignements auraient dû être transmis au ministre afin de répondre à ses attentes.

Dans mon rapport au ministre de la Défense nationale, j'ai également recommandé que le CSTC adopte des méthodes plus rigoureuses pour évaluer l'importance des renseignements étrangers fournis à leurs clients.

### Recommandations

En ce qui concerne les attentes relatives aux communications privées, j'ai recommandé au CSTC d'élaborer un énoncé explicite relatif à chaque attente ministérielle dans les rapports qu'il présentera au ministre. Je suis heureux de constater que le CSTC a accepté cette recommandation.



En outre, les membres de mon équipe ont signalé certaines irrégularités liées aux politiques et aux procédures du CSTC relatives aux activités examinées.

### Recommandations

Par suite de ces constatations, j'ai recommandé au CSTC d'adopter et de publier des directives écrites supplémentaires touchant les procédures que doivent suivre ses analystes lorsqu'ils prennent des décisions relativement aux cibles. J'ai également conseillé au CSTC de modifier sa politique en matière de radiation des communications privées qui, selon les analystes, n'ont aucune valeur sur le plan des renseignements étrangers. La LDN stipule que les communications privées interceptées ne seront utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité (alinéa 273.65(2)d).

Je suis heureux de constater que le CSTC a accepté mes recommandations et apporté des améliorations dans les domaines où nous avons relevé des carences, notamment la modification de ses systèmes.

## Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une autorisation ministérielle (activité 2)

### Contexte

Cet examen touchait certaines autres activités de collecte de renseignements étrangers menées par le CSTC en vertu de quatre autorisations ministérielles en vigueur de 2004 à 2007, y compris l'échange par le CSTC de renseignements étrangers à ses partenaires au Canada et à l'étranger.

### Conclusions

Selon les renseignements examinés et les entrevues, j'ai conclu que les activités étaient autorisées et conformes à la loi ainsi qu'aux politiques et aux procédures opérationnelles du CSTC. Les entrevues ont permis

Selon la *Loi sur la défense nationale*, les activités de collecte de renseignements étrangers ne peuvent viser des Canadiens ou toute personne au Canada (alinéa 273.64(2)a) et doivent être soumises à des mesures de protection de la vie privée des Canadiens lors de l'utilisation et de la conservation des renseignements interceptés (alinéa 273.64(2)b).

# Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une autorisation ministérielle (activité 1)

## Contexte

Cet examen touchait certaines activités de collecte de renseignements étrangers menées par le CSTC en vertu de trois autorisations ministérielles successives en vigueur entre 2004 et 2007. On a pris en compte deux examens des mêmes activités, réalisés par mon bureau en 1995 et en 2005.

## Conclusions

À la lumière des renseignements examinés et des entrevues, j'ai conclu que les activités du CSTC avaient été autorisées et menées conformément à la loi, aux exigences ministérielles ainsi qu'aux politiques et procédures opérationnelles de l'organisme.

Cependant, il en est ressorti que l'imputabilité du CSTC au ministre serait meilleure s'il consignait et rapportait davantage d'information. Cette information concerne les renseignements étrangers que le CSTC collecte en vertu de son autorisation ministérielle et qu'il communique à ses principaux partenaires à l'extérieur du Canada. Mon bureau continuera d'examiner la question d'échange de renseignements sur les Canadiens. L'examen a également révélé qu'un protocole d'entente entre le CSTC et un ministère fédéral concernant ces activités devrait être mis à jour de sorte qu'il soit conforme aux pratiques actuelles. Dans l'intervalle, le CSTC a convenu de continuer à respecter les modalités de l'entente actuelle et à consigner toute nouvelle entente.

## POINTS SAILLANTS DE L'EXAMEN 2008-2009

Au cours de l'année de référence 2008-2009, mon bureau a effectué sept examens portant sur différents aspects des activités du CSTC, et ce, sous mon autorité comme le prévoient l'alinéa 273.63(2a) et le paragraphe 273.65(8) de la *Loi sur la défense nationale*.

Les examens avaient pour objectif principal d'évaluer, conformément à mon mandat, si les activités du CSTC respectaient la loi et en particulier si l'organisme est doté de mesures suffisantes pour protéger la vie privée des Canadiens. Je suis en mesure d'affirmer que les activités ayant fait l'objet d'un examen en 2008-2009 respectaient la loi.

En ce qui concerne les trois premiers examens présentés ci-après (activités 1, 2 et 3), pour lesquels je me suis penché sur diverses activités de collecte de renseignements étrangers menées en vertu d'autorisations ministérielles, je tiens à souligner de nouveau que ces examens sont fondés sur l'interprétation juridique que le ministère de la Justice a fournie au CSTC, en attendant que la *Loi sur la défense nationale* soit modifiée.

### Examens d'activités entreprises en vertu d'autorisations ministérielles — Éléments communs

En vertu de l'alinéa 273.64(1a) de la *Loi*, le CSTC a pour mandat d'acquiescer et d'utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignements. Pour chaque activité de collecte de renseignements étrangers menée par le CSTC examinée par mon bureau en 2008-2009, le CSTC a obtenu une autorisation ministérielle en vertu des paragraphes 273.65(1) et (2) de la *Loi* étant donné qu'il était possible qu'il intercepte, dans le cadre de ces travaux, des communications provenant du Canada ou destinées au Canada considérées comme des « communications privées » aux termes du *Code criminel*.

**Formulation des conclusions et des recommandations**

La comparaison de la preuve recueillie aux critères de l'examen préalablement établis débouche sur la formulation de conclusions et de recommandations utilisables. Les conclusions permettent de confirmer si l'examen a satisfait aux critères, ou, si ce n'est pas le cas, de révéler le niveau, la nature et l'importance des écarts observés. Le processus d'évaluation de la preuve recueillie au regard des critères est fondé sur des questions telles que : les conclusions sont-elles à la hauteur des attentes et des critères de l'examen? S'il y a une lacune, quelle en est la cause? Quelles en sont les conséquences probables? Peut-on corriger la situation?

**Pertinent** : il existe une relation claire et logique entre les renseignements obtenus et les objectifs et critères de l'examen. Si les renseignements ne sont pas pertinents, ils ne peuvent être utilisés comme preuve; *reproductible* : il est probable qu'on obtiendrait les mêmes résultats si toutes les étapes de l'examen étaient répétées; *valable* : l'information est bien ce qu'elle est censée être relativement à son contenu, à son origine et au moment où elle a été recueillie. En général, la preuve recueillie est suffisante lorsqu'on a assez d'éléments pour convaincre une personne raisonnable de la validité des observations et des conclusions de l'examen et de la pertinence des recommandations. Pour décider si le poids de la preuve est globalement suffisant, je dois tenir compte de la qualité de la preuve recueillie et du coût lié à l'obtention d'éléments supplémentaires par rapport aux avantages qu'ils apporteraient.

### Preuve d'examen — Qu'en est-il?

La preuve est constituée des renseignements et des données que l'on collecte et utilise à titre de fondements factuels pour formuler des conclusions et des recommandations au regard des critères de l'examen.

À mon avis, un aspect très important de chaque examen des activités du CSTC est de faire en sorte que toutes les constatations, conclusions et recommandations de mon bureau soient étayées par des preuves solides. Autrement dit, chaque élément recueilli doit être directement *pertinent*, *reproductible* et *valable*.



## Cibler les risques pour la légalité et la vie privée

Pour élaborer un processus solide de sélection des examens, il est important de cerner les activités, les pratiques et les procédures qui risquent de compromettre le respect de la loi par le CSTC. Par exemple, il arrive que mon équipe repère des risques éventuels à partir d'exams des activités du CSTC qui sont terminés ou en cours ou lors des séances d'information que donne l'organisme. En outre, le CSTC peut lui-même détecter des risques éventuels.

Lorsque j'évalue des sujets pouvant faire l'objet d'un examen, je demande à mon équipe de se pencher sur des questions comme : à quel point le CSTC est-il exposé au risque d'activités illégales dans ce secteur et quelle est la probabilité que cela survienne? Et si cela survient, quelle en est l'incidence négative probable?

Par ailleurs, en 2008–2009, mon équipe a défini des critères détaillés permettant d'établir l'ordre de priorité dans lequel il examinera les risques éventuels. Ces critères, qui font continuellement l'objet d'améliorations, sont notamment les suivants : des modifications importantes des pouvoirs conférés par la loi; des modifications de la technologie; le fait qu'un secteur n'ait jamais fait l'objet d'un examen approfondi ou qu'il n'ait pas été examiné au cours des quatre dernières années; le suivi d'une recommandation faite auparavant; et des problèmes qui surviennent dans le domaine public.

## Caractéristiques d'un bon examen

Dans le cadre d'un examen, mon personnel examine tous les dossiers, fichiers, correspondance et autres documents écrits et électroniques se rapportant à l'activité en question. Il s'entretient avec les gestionnaires et les employés du CSTC qui ont participé aux activités visées par l'examen et se rend dans les locaux de l'organisme afin de procéder à des vérifications, y compris celles de ses bases de données. Les résultats de l'examen sont présentés au CSTC qui, dans la plupart des cas, prend des mesures afin de renforcer son respect de la loi ou des politiques.



## Mise en œuvre des recommandations — Qu'en est-il?

Depuis 1997, mon bureau a présenté 52 rapports au ministre. La plupart de ceux-ci comportaient nombre de recommandations. Le CSTC a accepté et mis en œuvre (ou il travaille à appliquer) plus de 90 p. 100 de ces recommandations, ce qui témoigne de l'efficacité du processus d'examen.

Lorsqu'ils procèdent à un examen, les membres de mon équipe approfondissent parfois beaucoup leurs recherches et vont observer directement les opérateurs et les analystes du CSTC, afin de mieux comprendre leur travail. Ces connaissances sont particulièrement importantes lorsqu'ils examinent un élément au sujet duquel j'ai fait une recommandation avec laquelle le CSTC est en désaccord. Une telle situation s'est présentée cette année — il en est question à la section Points saillants de l'examen — et j'ai révisé une recommandation sur la vie privée que j'avais formulée l'année dernière. Ainsi, à la suite d'un deuxième examen approfondi, j'ai rétracé ma recommandation parce que j'ai été convaincu que le risque pour la vie privée était minime et que le CSTC disposait de mesures de protection adéquates. Je pense que cette rétractation découle d'une approche rigoureuse, mais juste, en matière d'examen qui, dans ce cas, reconnaît le professionnalisme que s'efforcent d'appliquer les analystes concernés.

## Un processus d'examen approfondi

Il a pris des mesures positives afin de combler ses lacunes en la matière. En fait, un nouveau système ministériel de gestion des dossiers devrait être mis en place au cours de l'année de référence 2009-2010. Le CSTC mérite des éloges pour ses efforts dans ce secteur important.

## Exposés du CSTC

Le CSTC fournit régulièrement à mon bureau des exposés sur ses politiques opérationnelles et ses activités administratives pertinentes. En 2008–2009, mon bureau a également eu droit à des présentations et à des formations dans les domaines des bases de données relatives à la gestion de l'information et aux technologies de l'information (TI), sur la protection des réseaux TI importants pour le gouvernement du Canada et sur l'état des politiques du CSTC. Le CSTC a en outre donné des exposés particuliers à certains examens, avant le début de ces examens.

## des examens

### Table ronde annuelle à l'appui de l'efficacité

Au cours des deux dernières années, mon équipe et des représentants du CSTC ont participé à ce qui est devenu une table ronde annuelle destinée à optimiser le processus d'examen tout en réduisant les conséquences négatives sur les activités du CSTC prévues par la loi. Cette réunion est aussi l'occasion de renforcer une communication transparente et d'améliorer la compréhension et la confiance mutuelles dans la relation de travail entre les deux organisations. Ces réunions ont permis d'éliminer des obstacles à l'efficacité des examens et nous permettront, j'en suis convaincu, de réaliser des progrès au cours des années à venir.

### Renforcement du respect de la loi

Mon mandat d'examen a pour objectif d'évaluer si les activités du CSTC respectent la loi et si l'organisme est doté de mesures suffisantes pour protéger la vie privée des Canadiens. Je suis naturellement tenu d'informer le ministre et le procureur général du Canada de toute situation de non-conformité à la loi. Cependant, je me fais aussi un devoir de proposer, aussi souvent que possible, des mesures préventives visant à renforcer le respect de la loi par le CSTC.

La question de l'amélioration des pratiques de gestion de l'information en est une pour laquelle mes prédécesseurs et moi-même avons invariablement demandé que des mesures préventives soient prises. Comme nous l'avons tous indiqué, l'absence d'un système approprié de gestion des documents a entravé le CSTC dans sa capacité de rendre compte de ses activités.

## Protection de la vie privée : Examen périodique des divulgations d'identités

En décembre 2008, mon bureau a achevé un examen approfondi des activités du CSTC concernant la divulgation de renseignements sur les Canadiens aux clients du gouvernement du Canada. À la suite de cet examen, le CSTC a suggéré que mon bureau procède à un examen de ce genre de façon régulière. Puisque cette activité du CSTC est au cœur de mon mandat, je crois qu'il vaut la peine de la soumettre à un examen périodique. Mon bureau a donc pris les dispositions nécessaires avec le CSTC afin que l'on procède à des examens à intervalles réguliers au cours de l'année de référence à venir.

Je suis d'avis que la nature de cette suggestion du CSTC, tout comme la manière dont elle a été présentée à mon bureau, témoigne de la confiance professionnelle qui s'est développée dans la relation entre nos organismes respectifs. Il s'agit là d'un signe positif que je souligne avec plaisir dans ce rapport.

## Renseignements sur les Canadiens — Qu'en est-il?

Lorsqu'il collecte des renseignements étrangers, le CSTC peut, par inadvertance, obtenir des renseignements au sujet de Canadiens. Il peut conserver ces renseignements s'il estime qu'ils sont essentiels à la compréhension des renseignements étrangers. Pour inscrire ces renseignements dans des rapports de renseignements étrangers, il doit les supprimer (p. ex., en les remplaçant par un terme générique, comme « un Canadien ou une Canadienne »). Par la suite, s'il reçoit une demande de divulgation des renseignements supprimés, le CSTC exige du ministère ou de l'organisme fédéral qu'il rende compte de son pouvoir de demander et d'utiliser ces renseignements dans le cadre de son mandat et qu'il fournisse une justification opérationnelle de son besoin de connaître ces renseignements. Le demandeur doit satisfaire à toutes ces conditions avant que le CSTC divulgue les renseignements supprimés.

## Participation du comité parlementaire

à une telle collaboration des organismes d'examen, pourvu que celle-ci soit mise en œuvre de manière à respecter les exigences de sécurité, notamment la *Loi sur la protection de l'information*. Par ailleurs, je peux procéder, et je procède à l'examen des activités du CSTC dans le cadre de la troisième partie de son mandat, qui consistent à répondre aux demandes d'assistance du Service canadien du renseignement de sécurité (SCRS) et de la GRC, afin de vérifier si elles sont menées en conformité à la loi.

La commission d'enquête O'Connor comportait également un examen de la mise en commun de renseignements entre les organismes de différents pays. Cette question a déjà été discutée par des spécialistes du Canada et d'ailleurs. Lors de la conférence annuelle de l'Association canadienne pour les études de renseignement et de sécurité, en octobre 2008, il a été question d'un « manque d'imputabilité », du fait de l'absence de coopération entre les organismes d'examen de différents pays dans le cadre de l'examen des ententes d'échange de renseignements entre leur organisme de renseignement respectif. Bien qu'il s'agisse d'une question délicate, elle m'intéresse particulièrement, surtout parce qu'elle concerne l'éventuelle transmission de renseignements personnels sur les Canadiens. Je procéderai, dans le cadre de mes propres pouvoirs, à un examen des activités du CSTC dans ce secteur au cours de la prochaine année.



## Une réserve relative à l'examen

Au terme de l'année de référence 2008-2009, je continue d'appliquer la solution *temporaire* mise en place par mes prédécesseurs, soit de procéder à l'examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'autorisations ministérielles conformément à l'interprétation de la LDN du ministère de la Justice. Mais, à certains égards importants, tout comme mes deux prédécesseurs, je ne suis pas d'accord avec cette interprétation.

Dans son dernier rapport en tant que commissaire du CST en avril 2006, mon prédécesseur immédiat avait écrit : « Mon seul regret serait peut-être de devoir quitter mon poste avant qu'aient pu se régler les problèmes d'interprétation juridique qui compromettent la bonne marche des activités de ce bureau depuis décembre 2001 ». Dans mon rapport de 2007-2008, j'ai noté que le gouvernement avait indiqué que les modifications législatives seraient adoptées « en temps opportun ». Ceci n'a pas encore été fait. Mais je tiens à souligner que le temps qui s'écoule sans qu'on applique les modifications législatives met en danger l'intégrité du processus d'examen.

## Observations de la vérificatrice générale

Je suis heureux de constater que la vérificatrice générale a commenté cette question importante. Dans son rapport publié le 31 mars 2009, elle reconnaît que la réserve exprimée par le commissaire du CST au sujet de la légalité des activités du CSTC, en raison des ambiguïtés dans la loi le régissant, « a de sérieuses retombées » (*Rapport Le Point de 2009 de la vérificatrice générale du Canada*, mars, section 1.14).

## Collaboration aux fins de l'examen

La question de savoir s'il est nécessaire de fusionner l'examen des opérations intégrées entre les organismes d'application de la loi et de collecte du renseignement — qui découlait du rapport du juge Dennis O'Connor sur un nouveau mécanisme d'examen des activités de la Gendarmerie royale du Canada (GRC) en matière de sécurité nationale — n'a pas été réglée en 2008-2009. Le juge O'Connor recommandait entre autres l'instauration de « passerelles législatives » à l'appui d'un examen intégré. Je ne vois aucun obstacle, juridique ou autre,



## Les autorisations ministérielles — Qu'en est-il?

L'autorisation ministérielle est une autorisation écrite du ministre de la Défense nationale, qui établit les conditions que doit respecter le CSTC pour ne pas contrevenir au *Code criminel* dans l'éventualité où il intercepterait par inadvertance des communications privées de Canadiens dans le cadre de sa collecte de renseignements étrangers ou de ses activités liées à la sécurité des technologies de l'information. Ces autorisations peuvent être approuvées ou renouvelées pour une période maximale d'un an.

d'examen

Assurer l'intégrité des activités du CSTC et du processus

*nationale*

Modifications proposées à la Loi sur la défense

CONTEXTE DE L'EXAMEN

Dans le rapport de l'année dernière, j'ai réitéré mes inquiétudes au sujet de certaines ambiguïtés dans la partie V.1 de la *Loi sur la défense nationale* (LDN) au sujet des activités de renseignement étranger que mène le CSTC en vertu d'une autorisation ministérielle. J'ai recommandé un certain nombre de modifications, dont une visant à préciser les termes *activité* et *catégorie d'activités*. J'ai également recommandé que soient ajoutés à la Loi une définition des termes *intercepter* et *interception*. J'ai donc présenté ces modifications à la LDN, de même que certaines autres, aux représentants gouvernementaux, parce que j'estime qu'ils sont importants.

Alors que mon premier mandat touche à sa fin, je suis heureux de constater que la confiance mutuelle et l'engagement envers des valeurs démocratiques ont nourri une relation de travail productive. Je salue le leadership dont a fait montre le CSTC dans son engagement à se conformer à la loi et à protéger la vie privée des citoyens.

Le présent rapport est le troisième que je publie à titre de commissaire du Centre de la sécurité des télécommunications. Le moment est bien choisi, selon moi, pour présenter la nature du travail qu'effectue mon bureau et la qualité des relations qui se sont établies entre ce dernier et le Centre de la sécurité des télécommunications Canada (CSTC).

Plusieurs dizaines d'années d'expérience dans le domaine juridique m'ont appris que l'élément le plus important d'une relation est la confiance. Cela est vrai pour toutes les relations, y compris celles qu'entretiennent mon bureau et le CSTC. D'après moi, la confiance n'est pas un droit. C'est quelque chose que l'on gagne par son intégrité et son professionnalisme. Le CSTC a gagné cette confiance en faisant la preuve d'un engagement envers la protection de la sécurité nationale et en s'acquittant de ce mandat dans le respect de la loi et de la vie privée des Canadiens. Pour mon bureau, la confiance est le fruit d'un processus d'examen rigoureux, approfondi et juste.

En raison de la nature de son travail, le CSTC doit exercer une grande partie de ses activités dans le secret. Le rôle de mon bureau consiste notamment à représenter l'intérêt public dans le cadre de la reddition de comptes d'une façon qui favorise un examen efficace sans toutefois compromettre sans raison la mission confiée au CSTC par la loi.

Mes prédécesseurs et moi-même avons toujours reconnu que la prévention est un aspect important du rôle confié au commissaire par la loi. De ce fait, la plupart de mes recommandations visent à corriger des lacunes en ce qui a trait aux politiques, aux procédures et aux pratiques du CSTC, afin de renforcer le cadre de conformité et de réduire les risques pour la vie privée. Au cours des trois dernières années, j'ai indiqué n'avoir trouvé aucun défaut de conformité à la loi. Cependant, il peut arriver (et cela s'est produit) que je sois en désaccord avec le CSTC relativement à un point particulier ou que les justifications ou les renseignements donnés par l'organisme ne me satisfassent pas. Dans ces cas, je demande à mon équipe d'examiner la question aussi attentivement qu'il le faut. La façon dont ces questions sont abordées peut raffermir la confiance professionnelle entre les deux organisations.

- Suivi d'une recommandation découlant de l'examen effectué en vertu d'une directive ministérielle / 18
- Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une directive ministérielle et à l'appui de son mandat en matière de collecte de renseignements étrangers / 19

Examens en cours ou projetés / 20

Plaintes au sujet des activités du CSTC / 21

Fonctions exercées en vertu de la Loi sur la protection de l'information / 22

- Le bureau du commissaire / 22
- Nouveau statut de mon bureau / 22
  - Conférence 2008 de l'Association canadienne pour les études de renseignement et de sécurité / 23
  - Conférence internationale des organismes de surveillance du renseignement / 23
  - British Intelligence and Security Committee of Parliamentarians / 24

Mot de la fin / 24

Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications / 25

Annexe B : Rapports classifiés au ministre, 1996–2009 / 27

Annexe C : Etat des dépenses, 2008–2009 / 31

Annexe D : Historique du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) / 33

Annexe E : Rôle et mandat du Centre de la sécurité des télécommunications Canada (CSTC) / 35

Annexe F : Programme d'examen du BCCST — Modèle logique / 37

- Modifications proposées à la *Loi sur la défense nationale* / 2
- Assurer l'intégrité des activités du CSTC et du processus d'examen / 2
- Une réserve relative à l'examen / 3
- Observations de la vérificatrice générale / 3
- Collaboration aux fins de l'examen / 3
- Participation du comité parlementaire / 4

- Protection de la vie privée : Examen périodique des divulgations d'identités / 5
- Exposés du CSTC / 6
- Table ronde annuelle à l'appui de l'efficacité des examens / 6
- Renforcement du respect de la loi / 6
- Un processus d'examen approfondi / 7

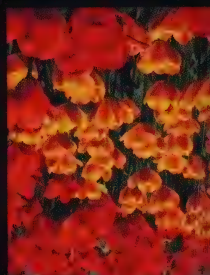
- Cibler les risques pour la légalité et la vie privée / 8
- Caractéristiques d'un bon examen / 8
- Formulation des conclusions et des recommandations / 8

- Examens d'activités entreprises en vertu d'autorisations ministérielles — Éléments communs / 10
- Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une autorisation ministérielle (activité 1) / 11
- Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une autorisation ministérielle (activité 2) / 12
- Examen des activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une directive ministérielle et d'une autorisation ministérielle (activité 3) / 14
- Examen de l'acquisition et de la mise en œuvre des technologies par le CSTC comme moyen de protéger la vie privée des Canadiens / 15
- Examen de la divulgation de renseignements sur les Canadiens aux clients du gouvernement du Canada / 17





2008-2009



# Rapport annuel

COMMISSAIRE  
DU CENTRE  
DE LA SÉCURITÉ  
DES TÉLÉCOMMUNICATIONS



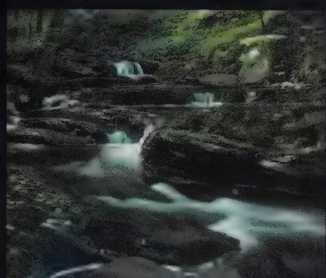
CA1  
ND 800  
- S16



Government  
Publications

COMMUNICATIONS  
SECURITY  
ESTABLISHMENT  
COMMISSIONER

# Annual Report



2009-2010

Canada

Office of the Communications Security  
Establishment Commissioner  
P.O. Box 1984, Station "B"  
Ottawa, Ontario  
K1P 5R5

Tel.: (613) 992-3044  
Fax: (613) 992-4096  
Website: [www.ocsec-bccst.gc.ca](http://www.ocsec-bccst.gc.ca)

© Minister of Public Works and  
Government Services Canada 2010  
ISBN 978-1-100-51826-8  
Cat. No. D95-2010

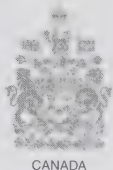
Cover photos: Malak



**Mixed Sources**  
Product group from well-managed  
forests and other controlled sources  
[www.fsc.org](http://www.fsc.org)  
Cert no. SGS-COC-005437  
© 1996 Forest Stewardship Council

Communications Security  
Establishment Commissioner

The Honourable Robert Décary, Q.C.



Commissaire du Centre de la  
sécurité des télécommunications

L'honorable Robert Décary, c.r.

June 2010

Minister of National Defence  
MGen G.R. Pearkes Building, 13<sup>th</sup> Floor  
101 Colonel By Drive, North Tower  
Ottawa, Ontario  
K1A 0K2



Dear Sir:

Pursuant to subsection 273.63(3) of the *National Defence Act*, I am pleased to submit to you the annual report for the period of April 1, 2009, to March 31, 2010, on the activities and findings of my two predecessors, the Honourable Peter deC. Cory and the late Honourable Charles D. Gonthier, for your submission to Parliament.

Yours sincerely,

Robert Décary

*This report is dedicated to the memory of*

The Honourable Charles D. Gonthier, C.C., Q.C.

1928–2009



---

## TABLE OF CONTENTS

Introduction /1

Review Environment /2

- Proposed amendments to the *National Defence Act* /2
- CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act* /5
- Findings and recommendations arising from the Iacobucci and O'Connor inquiries /6

Year In Review /8

- Regular review of disclosures of information about Canadians /9
- Timeliness of CSEC's responses to information requests /9
- Enabling a higher level of assurance /9
- Strengthening accountability and compliance /10

Review Methodology /11

- Review criteria /11
- A new approach to reviewing foreign intelligence activities /12

2009–2010 Review Highlights /14

- Study of CSEC information technology security activities not conducted under ministerial authorization /14
- Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations and in support of government efforts relating to Afghanistan /17
- Regular review of CSEC disclosure of information about Canadians to Government of Canada clients /19

Work Plan — Reviews Underway And Planned /21

- Current reviews /22
- Upcoming reviews /22

Complaints about CSEC's Activities /22

---

Duties Under The *Security Of Information Act* /23

The Commissioner's Office /23

- Comparative study of CSEC and international partners /23
- Canadian Association of Security and Intelligence Studies (CASIS) conference /24
- International Intelligence Review Agencies Conference (IIRAC) /24

In Closing /25

A Tribute to the Honourable Charles Doherty Gonthier, C.C., Q.C. /25

Annex A: Mandate of the Communications Security Establishment Commissioner /27

Annex B: Classified Reports to the Minister /29

Annex C: Statement of Expenditures 2009–2010 /33

Annex D: History of the Office of the Communications Security Establishment Commissioner /35

Annex E: Role and Mandate of the Communications Security Establishment Canada (CSEC) /37

Annex F: Commissioner's Office Review Program — Logic Model /39

---

## INTRODUCTION

**By the Honourable Peter deC. Cory, C.C., C.D.**

I was pleased to accept the appointment of Communications Security Establishment Commissioner, effective December 14, 2009. The office had been without a Commissioner since the untimely death last July of my predecessor, and former colleague on the Supreme Court of Canada, the late Honourable Charles D. Gonthier.

Upon my arrival at the office last December, what impressed me immediately was the professionalism and dedication of the staff. Despite the fact that there had been no Commissioner in place between the passing of Mr. Gonthier and my appointment, the work of the office continued, with staff carrying on review of the Communications Security Establishment Canada (CSEC) activities. The only work that did not proceed was the forwarding of review reports to the Minister, a task which is the sole responsibility of the Commissioner.

I was also struck by the professionalism and dedication of CSEC personnel. One area of activity in 2009–2010 which stands out is CSEC’s important, and at times life-saving, work in support of Canadian Forces in Afghanistan, as a priority established by the Government of Canada.

During the time between my appointment and the end of this reporting period, I was thoroughly apprised of CSEC’s activities through a comprehensive briefing from the Chief of CSEC as well as briefings and discussions with my staff pertaining to the review of CSEC’s activities to assess compliance with relevant legislation.

I know from past reports that those CSEC activities that were reviewed complied with the law. The opportunity I had for discussions with the Chief and with my staff demonstrated to me that there is consistency in the way in which CSEC fulfills its mandate. Those activities about which I submitted reports to the Minister of National Defence also complied with the law. This is a reflection of a culture of compliance

---

that exists within CSEC.

This is not to say that there are not certain issues about which there are or may be disagreements. These disagreements can be worked through more effectively, however, when there is a fundamental understanding of the law by CSEC staff and a practical appreciation of how it applies to their work.

As a final word, let me state that subsequent to my appointment in late 2009, a number of factors intervened to lead me to limit my time as Commissioner. These are circumstances that I sincerely regret, since the process of selection must take time. However, life sometimes sets before us circumstances that do not always work out the way we would have thought or preferred. I am grateful for the opportunity I had to work with the able and conscientious staff at the Commissioner's office. I am assured as well that my successor has a sound base on which to carry forward the important, independent role of the Commissioner in ensuring that CSEC complies with the law and protects the privacy of Canadians while fulfilling its legislated mandate.

## REVIEW ENVIRONMENT

### **Proposed amendments to the *National Defence Act***

The *National Defence Act* (NDA) prohibits CSEC from directing its foreign intelligence and information technology security activities at a Canadian or any person in Canada. It also requires CSEC to take measures to protect the privacy of Canadians in the use and retention of intercepted information.

---

However, due to the manner in which communications are transmitted, CSEC may, while conducting its mandated foreign intelligence collection or information technology security activities, unintentionally intercept communications of Canadians or persons in Canada, which constitute “private communications” as per section 183 of the *Criminal Code*.

Recognizing this possibility, the *NDA* allows the Minister of National Defence to authorize CSEC to intercept private communications. Prior to granting this authorization, however, the Minister must be satisfied that certain conditions set out in the *NDA* are met. There are four conditions for foreign intelligence collection ministerial authorizations (subsection 273.65(2)) and five conditions for information technology security ministerial authorizations (subsection 273.65(4)).

CSEC’s activities conducted under a ministerial authorization must be undertaken in accordance with:

- relevant legislation, namely the *NDA*, *Canadian Charter of Rights and Freedoms*, *Privacy Act*, *Criminal Code*, as well as Justice Canada advice;
- requirements set out by the Minister of National Defence in the authorization or in a ministerial directive, for example, for accountability, to record and report to the Minister certain information after the expiration of the ministerial authorization; and
- CSEC policies and procedures.

Part of the Commissioner’s legislated mandate is to examine CSEC’s activities under ministerial authorizations to ensure they were authorized and conducted in compliance with the law. Reviews by past Commissioners have never identified an instance in which CSEC targeted the communications of a Canadian or a person in Canada.



## Private communications and information about Canadians

Reviews of CSEC activities under ministerial authorizations have consistently demonstrated that the proportion of private communications of Canadians that CSEC unintentionally intercepts is very small.

CSEC's classified foreign intelligence reports may contain information about Canadian citizens, permanent residents or Canadian corporations (as defined in section 273.61 of the *NDA*), if such information is deemed essential to the understanding of the reports. However, this information must be suppressed, that is replaced by a generic reference such as "a Canadian person".

CSEC's foreign intelligence ministerial authorizations are broadly written and apply to methods of collecting foreign intelligence rather than to individuals. However, Commissioners have been of the view that it is not clear that the *NDA* supports such an approach. Commissioners have stated that amendments to the *NDA* are necessary to clarify ambiguities relating to foreign intelligence ministerial authorizations. Former Commissioner Gonthier also emphasized last year that "the length of time that has passed without producing amended legislation puts at risk the integrity of the review process."

Commissioner Gonthier was informed by the Minister of National Defence that clarification of ambiguities and other amendments to the *NDA* are a legislative priority. Pending amendments, Commissioners have continued to use the interim solution of applying a qualified opinion, that is, reviewing CSEC foreign intelligence collection activities under ministerial authorization on the basis of the *NDA* as it is interpreted by Justice Canada. However, past Commissioners have noted they disagree in certain important respects with that interpretation, which highlights the need for amendments to the *NDA*.

---

## CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act*

National security matters are increasingly the subject of court and other public proceedings. In his October 5, 2009 decision in the matter of an application for a warrant pursuant to sections 12 and 21 of the *CSIS Act*, the Honourable Mr. Justice Mosley of the Federal Court authorized CSIS, with the technical assistance of CSEC, to intercept from *within* Canada communications pertaining to threat-related activities in which it was believed two persons would engage while travelling *outside* of Canada. Justice Mosley distinguished the application from a similar one heard and denied in October 2007 by the Honourable Mr. Justice Blanchard, also of the Federal Court.

In the reasons for his decision, Justice Mosley emphasized that “[i]n authorizing CSIS, with the technical assistance of CSE[C], to collect information ... intercepted in Canada, I am not authorizing CSE[C] to overstep its legislative mandate under the *National Defence Act*. [...] CSE[C] will not be directing its activities at Canadian citizens to acquire information for its purposes but assisting CSIS”.

### **CSEC's mandate to assist federal law enforcement and security agencies**

Paragraph 273.64(1)(c) of the *National Defence Act* permits CSEC to provide technical and operational assistance to federal law enforcement and security agencies. CSEC is subject to any limitations imposed by law on the agency to which CSEC is providing assistance — for example, conditions imposed by a judge in a warrant.

---

In 2010–2011, the Commissioner’s office will conduct a review of CSEC’s assistance to CSIS involving the interception in Canada of communications of Canadians located outside of Canada and subject to a warrant under sections 12 and 21 of the *CSIS Act*, such as those authorized by Justice Mosley’s decision.

## Findings and recommendations arising from the Iacobucci and O’Connor inquiries

In June 2009, the House of Commons Standing Committee on Public Safety and National Security issued a report of its review of the findings and recommendations arising from the *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (Iacobucci inquiry) and the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (O’Connor inquiry). The Standing Committee urged the government to implement all of the recommendations from these inquiries.

In October 2009, the government responded to the Standing Committee’s report with a commitment “...to modernize and strengthen the national security review framework”. Specifically, the response stated: “[t]he Government’s objective is to strengthen national security structures that are already in place...” and “[m]uch work has also been done to advance policy analysis on Canada’s national security review framework ” including “...providing a mechanism to facilitate inter-agency review of national security activities”.

Regarding the latter point, former Commissioner Gonthier stated that there are no obstacles, legal or otherwise, to cooperation among national security review agencies. Much can be done by way of joint or parallel reviews, research or other collaborative work.

Respecting the role of parliamentarians, and in the context of the development of an enhanced national security framework, the government's response indicated that due consideration will be given to the Standing Committee's fifth recommendation: that Bill C-81, introduced in the 38<sup>th</sup> Parliament, *An Act to Establish the National Security Committee of Parliamentarians*, or a variation of it, be introduced in Parliament at the earliest opportunity. Past Commissioners have raised questions about the composition of such a committee and its access to classified national security information.

The O'Connor and Iacobucci inquiries also identified a number of issues respecting Canadian security and intelligence agencies' sharing of information with foreign agencies. The government's response indicated that "[t]he cumulative result of successive commissions of inquiry, reports and lessons learned has been the refinement of policies and practices surrounding the exchange of information between foreign partners and Canada's national security and intelligence and law enforcement communities". Information sharing is an essential component of CSEC's foreign intelligence program. The Commissioner's office is currently completing a review of this activity.

In its response to the recommendations of the O'Connor and Iacobucci inquiries, the government indicated that it will continue to consider the advice of stakeholders. The Commissioner's office remains willing to discuss such matters.



## YEAR IN REVIEW

The last reporting year was a unique one for the Commissioner's office. As noted in the introduction, there was no Commissioner for a period of five months following the passing of Commissioner Gonthier. Nevertheless, the work of the office continued. Reviews and classified reports were completed, and others that had been approved by former Commissioner Gonthier were continued, or begun, as planned.

The primary objective of reviews is to assess whether CSEC's activities comply with the law, including the extent to which adequate measures are in place to protect the privacy of Canadians. Three classified reports were submitted to the Minister during the past year. One was a comprehensive study relating to CSEC information technology security activities and two were reviews relating to foreign intelligence activities.

The two reviews found that CSEC complied with the law and ministerial requirements and protected the privacy of Canadians. CSEC accepted the recommendations made in the reviews and is taking action to address them. CSEC is also addressing findings in order to improve its policies or practices.

### Implementing recommendations

Since 1997, Commissioners have submitted to the Minister of National Defence 55 classified review reports and studies. In total, these reports have contained 129 recommendations. CSEC has accepted and implemented or is working to address 94 percent (121) of these recommendations. The few recommendations that were not accepted or implemented may have been in areas surpassed by events or circumstances. In an instance where CSEC rejects a recommendation, the Commissioner reviews the reasons provided by CSEC, then assesses whether to accept these reasons or to pursue the issue, possibly by examining it in even greater depth.



---

## Regular review of disclosures of information about Canadians

The Commissioner's 2008–2009 annual report noted that the Commissioner's office would conduct regular reviews of CSEC's disclosure of information about Canadians to Government of Canada clients. For a period of six months last year, the Commissioner's office conducted monthly reviews of all disclosures and found them to comply with the law, and with CSEC policies and procedures. Given these positive results as well as the positive result of a more comprehensive review of disclosures reported in the 2008–2009 annual report, it was determined that monthly reviews were not necessary. However, given also that this activity lies at the heart of the Commissioner's mandate, as noted by former Commissioner Gonthier last year, an annual review will still be conducted.

## Timeliness of CSEC's responses to information requests

CSEC's operations in 2009–2010 were affected by a number of extraordinary factors and external pressures such as responding to international special events. While Commissioners respect that operations must be CSEC's priority, the length of time CSEC took to respond to requests for information from the Commissioner's office this past year was at times too long. CSEC is examining ways to better support the Commissioner's review requirements.

## Enabling a higher level of assurance

During the past year, CSEC provided a number of detailed briefings to staff of the Commissioner's office. Some of the briefings were general in nature with the objective of keeping the office informed of operational, policy and organizational issues. Other briefings provided information on specific CSEC activities prior to establishing terms of reference for a review or during a review underway.

---

Several briefings described CSEC's tools, systems and databases, including those used to ensure that CSEC complies with statutory requirements for targeting foreign entities outside of Canada.

The briefings, along with direct access to CSEC systems and front-line employees, enhanced the depth of review by the Commissioner's office in 2009–2010. All of this enables a Commissioner to provide a higher level of assurance to the Minister of National Defence that CSEC is complying with the law and protecting the privacy of Canadians.

### **Strengthening accountability and compliance**

Commissioners look to reinforce good practices that maintain or strengthen CSEC's compliance with the law and the protection of the privacy of Canadians. CSEC has continued to make significant improvements to its information management practices and has continued to expand the use of its corporate records management system, issues that were subjects of past recommendations by Commissioners. These enhancements are critical to CSEC accountability and compliance.

CSEC is also to be commended for a new initiative to increase employee awareness and knowledge of the authorities, policies and procedures governing its activities. This initiative makes policies which are specifically relevant to an employee's position readily available on the employee's computer. This initiative is expected to strengthen CSEC's compliance framework and the protection of the privacy of Canadians.

---

## REVIEW METHODOLOGY

In the conduct of a review, the Commissioner's staff examine relevant written and electronic records, files, correspondence and other documentation, including policies, procedures and legal advice. CSEC provides briefings and demonstrations of its activities as well as detailed answers in response to written questions from the Commissioner's office.

Commissioner's staff may test the information obtained against the contents of CSEC systems and databases. In addition, Commissioner's staff interview CSEC managers and other personnel involved in activities under review and observe firsthand CSEC operators and analysts to learn exactly how they are conducting their work.

The Commissioner's office may also refer to the work of CSEC's internal auditors and evaluators. In some cases, this may lead to identifying an activity for review.

### Review criteria

Reviews conducted by the Commissioner's office include an assessment of CSEC's activities against a standard set of criteria respecting legal requirements, ministerial requirements, and CSEC policies and procedures. Other criteria may be added to each review, as appropriate.

**Legal requirements:** The Commissioner expects CSEC to conduct an activity in accordance with the *NDA*, the *Canadian Charter of Rights and Freedoms*, *Privacy Act*, *Criminal Code*, any other relevant legislation and Justice Canada advice.

**Ministerial requirements:** The Commissioner expects CSEC to conduct an activity in a manner that is in accordance with ministerial direction, namely any requirements and limitations set out in a ministerial authorization or directive.

**Policies and Procedures:** The Commissioner expects CSEC to have appropriate policies and procedures in place to guide an activity and to provide sufficient direction respecting legal and ministerial requirements and the protection of the privacy of Canadians. The Commissioner expects CSEC employees to be aware of and comply with policies and procedures. The Commissioner also expects CSEC to utilize an effective management control framework to ensure that the integrity and lawful compliance of an activity is maintained on a routine basis. This includes appropriate accounting for decisions taken and for information relating to compliance and the protection of the privacy of Canadians.

## **A new approach to reviewing foreign intelligence activities**

CSEC's foreign intelligence collection activities conducted under ministerial authorization involve a number of distinct methods of acquiring information from the global information infrastructure. Nevertheless, there are a number of common processes and associated tools, as well as common systems and databases, which support these collection methods and which CSEC uses to deal with the information obtained. For example, common to all of the collection methods are the processes by which CSEC: selects foreign entities located outside Canada that are of foreign intelligence interest; shares reports and information with its clients and international partners; and retains or disposes of intercepted communications.



Rather than examine thoroughly individual ministerial authorizations, it was assessed as more effective to examine thoroughly each process common to CSEC's foreign intelligence collection activities under ministerial authorization. This new approach, which cuts across the collection methods, is referred to as *horizontal review*.

## Why horizontal review?

The horizontal review approach, born of years of accumulated review experience on the part of the Commissioner's office, is designed to provide the Commissioner's staff with an even more comprehensive understanding of how CSEC conducts its activities. Ultimately, its objective is to increase the degree of assurance the Commissioner can provide to the Minister of National Defence that CSEC is complying with the law and protecting the privacy of Canadians.

In addition to the horizontal review approach, the Commissioner's office now reviews all foreign intelligence ministerial authorizations together, on an annual basis. This review will identify any significant changes to the activities covered by the ministerial authorizations or in the authorizations themselves. Any significant changes will be assessed in terms of their impact on risks of non-compliance and risks to the privacy of Canadians. If appropriate, a detailed review will be conducted. This annual review of foreign intelligence ministerial authorizations will also examine used and retained intercepted private communications to ensure they are communications essential to international affairs, defence or the security of Canada, as required by paragraph 273.65(2)(d) of the *NDA*.



---

## 2009-2010 REVIEW HIGHLIGHTS

The Commissioner provides classified reports containing findings and recommendations to the Minister of National Defence, with copies going to the Chief of CSEC, to the National Security Advisor to the Prime Minister, who is accountable for CSEC operations and policy, and to the Deputy Minister of National Defence, who is accountable for administrative matters pertaining to CSEC. Prior to finalizing a report, the Commissioner's office seeks CSEC's comments respecting the report's factual accuracy.

### Study of CSEC information technology security activities not conducted under ministerial authorization

#### Background

This study was initiated and conducted under the authority of former Commissioner Gonthier, as articulated in paragraph 273.63(2)(a) of the *NDA*. It examined CSEC information technology (IT) security activities not conducted under ministerial authorization. A previous review of IT security activities was conducted in 2000. However, because of significant changes and developments in this area since that time, a comprehensive study was undertaken of all IT security activities not conducted under ministerial authorization. Other IT security activities that CSEC conducts under ministerial authorizations are reviewed annually.

CSEC's principal authority for IT security is derived from paragraph 273.64 (1)(b) of the *NDA*: "to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada". CSEC's IT security activities focus on preventing and responding to sophisticated IT threats and cyber attacks that attempt to covertly access sensitive government computer systems. Among its IT security activities, CSEC promotes sound security practices to help government departments reduce IT vulnerabilities and manage IT security risks. This may involve

---

the provision of monitoring and countermeasures to prevent, detect and respond to IT threats and cyber attacks.

The objectives of the study were to acquire knowledge of CSEC IT security activities and to conduct a risk assessment to determine which of these activities, if any, may raise issues about compliance with the law, ministerial requirements, CSEC policy and procedures, or the protection of the privacy of Canadians — and should therefore be subject to follow-up review. Particular attention was paid to activities that may involve private communications or information about Canadians.

Some of the areas included in the scope of this study were: the government's cryptographic program; relationships with industry; research, analysis and reporting respecting cyber vulnerabilities and sophisticated IT threats and attacks; assistance in identifying and responding to vulnerabilities and incidents affecting information infrastructures of importance to the government; and associated relationships with key Canadian government and international partners.

## Findings and conclusions

The study found that CSEC IT security activities not conducted under ministerial authorization generally present a low risk of possible non-compliance with Part V.1 of the *NDA* and a low risk to the privacy of Canadians. One quarter of the areas included in the study were identified for follow-up review and have been incorporated into the Commissioner's three-year work plan.

In only a few cases, CSEC's IT security activities not conducted under ministerial authorization involve access to a small amount of information about Canadians. Most of this information relates to the identity of a Canadian company, or consists of information voluntarily provided by CSEC's government clients as part of cyber protection activities or ongoing Crown business.

There are, however, other IT security activities not conducted under ministerial authorization that may present risks to the privacy of Canadians. These activities are conducted under the *Criminal Code* and the *Financial Administration Act* authorities of other government entities and may involve CSEC access to private communications and information about Canadians. In respect of these activities, the study found that CSEC takes measures to protect the privacy of Canadians. For example, private communications and information about Canadians are disclosed only to those officials involved in protecting computer systems. Nevertheless, the potential risks to privacy presented by these activities cannot be discounted. Therefore, the Commissioner's office will conduct in-depth reviews of these activities to verify CSEC's compliance, and to assess the extent to which it protects the privacy of Canadians in carrying out these activities.

### **Intrusion detection system monitoring**

Paragraph 184(2)(e) of the *Criminal Code* permits in part the interception of a private communication by a person in control of a computer system in order to protect the computer system from any act that would be an offence under subsections 342.1(1) ("unauthorized use of computer") or 430(1.1) ("mischief in relation to data") of the *Criminal Code*. This provision permits the use of an intrusion detection system to protect against a cyber attack and allows for the use or retention of a private communication where it is essential to identify, isolate or prevent harm to the computer system.

Section 161 of the *Financial Administration Act* provides authority for a government entity to take reasonable measures to protect a computer system, including the interception of a private communication in circumstances specified in paragraph 184(2)(e) of the *Criminal Code*.

---

The study also included the examination of a principal CSEC IT security software tool and information repository. Former Commissioner Gonthier concluded that the CSEC IT security software tool has adequate functionality to restrict access to information held in the system, to meet security and confidentiality requirements, and to protect the privacy of Canadians. To confirm this, the Commissioner's office examined CSEC's use of the system in the context of a review of certain IT security activities conducted under ministerial authorization. The results of this review will be included in the 2010–2011 annual report.

## **Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations and in support of government efforts relating to Afghanistan**

### **Background**

This review was initiated and conducted under the authority of former Commissioner Gonthier, as articulated in subsection 273.65(8) of the *NDA*. The report was reviewed and submitted to the Minister of National Defence by former Commissioner Cory. The review examined activities conducted under two ministerial authorizations in effect in 2006–2007 and 2007–2008 and in support of Canadian Forces military operations and other government efforts relating to Afghanistan. CSEC obtained the ministerial authorizations pursuant to subsections 273.65(1) and (2) of the *NDA* because, in carrying out the activities, it was possible that CSEC might intercept a communication that either originated or terminated in Canada, constituting a private communication, as defined in the *Criminal Code*.



Pending amendments to clarify the *NDA*, this review was based on the legal interpretation of the foreign intelligence ministerial authorization provisions in the *NDA* provided to CSEC by Justice Canada.

As this was the first review of these activities, the objectives were to acquire detailed knowledge of these activities, to assess whether these activities were authorized and complied with the law, and to assess the extent to which CSEC protected the privacy of Canadians in carrying out these activities.

## Findings

It is clear that CSEC's activities under ministerial authorization and relating to Afghanistan provide important access to valuable foreign intelligence that supports both military and broader government intelligence priorities.

The activities were found to have involved access to a minimal number of private communications and information about Canadians. They were therefore assessed as presenting a low risk to the privacy of Canadians.

Based on information reviewed and interviews conducted, CSEC activities from 2006–2008 under ministerial authorization and relating to Afghanistan were found to have been appropriately authorized and conducted in accordance with the law and Justice Canada advice. These activities were also found to have been conducted in accordance with requirements in the ministerial authorizations and with ministerial direction. CSEC recorded and reported information to the Minister in accordance with the requirements of the authorizations.



---

## Recommendations

No information or documentation was found to indicate that CSEC employees contravened operational policies and procedures applicable to these foreign intelligence collection activities. However, former Commissioner Gonthier recommended that CSEC amend its policy for these activities to clarify certain obligations. It is a positive development that CSEC acted on this recommendation and, as a result, has strengthened its ability to meet legal and ministerial requirements. The Commissioner's office will also monitor CSEC efforts to address gaps related to CSEC's dealings with the Canadian Forces, as identified by CSEC internal evaluators.

In addition, this review noted two CSEC enhancements related to foreign intelligence collection reporting that should be recognized. First, CSEC took action to centrally manage a certain type of reporting to enhance accountability for such reporting. Second, CSEC addressed a recommendation by former Commissioner Gonthier that additional information respecting foreign intelligence collection activities be recorded and reported to the Minister of National Defence to strengthen accountability.

## Regular review of CSEC disclosure of information about Canadians to Government of Canada clients

### Background

This review was initiated and conducted under the authority of former Commissioner Gonthier, as articulated in paragraph 273.63(2)(a) of the *NDA*. The report was reviewed and submitted to the Minister of National Defence by former Commissioner Cory.

When receiving a request for disclosure of the details of suppressed information about a Canadian in a report, CSEC requires its clients to explain their authority to obtain and use this information, and to provide an operational justification of their need for such information. Only after these conditions have been met will CSEC release the suppressed information.

The Commissioner's 2008–2009 annual report contained a summary of a comprehensive review of disclosure of information about Canadians to Government of Canada clients. The review found that CSEC activities complied with law, and with CSEC policies and procedures. Subsequently, CSEC suggested that reviews of this activity could be conducted at regular intervals. Recognizing that this CSEC activity is important to privacy protection, former Commissioner Gonthier agreed with CSEC's suggestion and monthly reviews of all CSEC disclosures to Government of Canada clients were conducted from January to June 2009.

## Findings

The monthly reviews found that CSEC's disclosure of information about Canadians in foreign intelligence reports to Government of Canada clients complied with the law and with CSEC operational policies and procedures. Given these positive results, it was determined that monthly reviews were not necessary and not the most effective use of resources for either party. However, given the privacy implications of this activity, commencing in 2010–2011, the Commissioner will conduct an annual review of a random sample of disclosures to verify that CSEC continues to comply with the law and maintains measures that protect the privacy of Canadians.

---

## Recommendations

Notwithstanding the positive findings, former Commissioner Gonthier made two recommendations respecting reporting to the Minister of National Defence on the volume of information about Canadians released to CSEC's clients. The recommendations relate to providing tools to support the tracking of such information and to improving the consistency and accuracy of the reporting. CSEC has accepted and is implementing the recommendations.

## WORK PLAN — REVIEWS UNDERWAY AND PLANNED

CSEC activities selected for review are prioritized using a set of detailed criteria. For example, the ongoing review of CSEC's foreign intelligence sharing with international partners was identified as a high-priority review topic. This is because: there have been changes to the authorities and technologies relating to these activities; the amount of foreign intelligence CSEC provides to and receives from its international partners is significant; these activities could directly and adversely affect a Canadian; specific and important controls are placed on the activities to ensure compliance with legal, ministerial and policy requirements, and these controls should be examined; and, finally, in past reviews relating to these activities, Commissioners have made findings and recommendations which require follow-up.

Decisions respecting the selection and prioritization of subjects for review are documented in the Commissioner's three-year work plan, which is updated regularly as part of an ongoing process of assessing risk.

---

## Current reviews

The results of several reviews currently underway are expected to be reported on to the Minister of National Defence in the coming year and included in the Commissioner's 2010–2011 public annual report.

The subjects of these reviews include: CSEC's foreign intelligence sharing with international partners; activities conducted under IT security ministerial authorizations; the process by which CSEC determines that targets of foreign intelligence interest are foreign entities located outside of Canada, as required by the *NDA*; a method used by CSEC to identify new entities believed to be of foreign intelligence interest; and an annual review of foreign intelligence ministerial authorizations, including a sample of associated private communications.

## Upcoming reviews

Other reviews planned for 2010–2011 include: assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the *CSIS Act*; an annual review of CSEC disclosures of information about Canadians to government clients and international partners; CSEC's retention and disposal of information, and, in particular, of private communications and information about Canadians; and CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 16 and 21 of the *CSIS Act*. Some reviews may carry over into the 2011–2012 fiscal year.

## COMPLAINTS ABOUT CSEC'S ACTIVITIES

The Commissioner's mandate includes undertaking any investigation deemed to be necessary in response to a complaint in order to determine whether CSEC has engaged, or is engaging, in unlawful activity.

In 2009–2010, correspondence was received concerning CSEC activities but none warranted investigation.



---

## DUTIES UNDER THE SECURITY OF INFORMATION ACT

The Commissioner has a duty under the *Security of Information Act* to receive information from persons who are permanently bound to secrecy seeking to defend the release of special operational information on the grounds that it is in the public interest. No such matters were reported to the Commissioner in the 2009–2010 reporting period.

## THE COMMISSIONER'S OFFICE

Last year, the Commissioner's office was granted its own appropriation from Parliament, strengthening the Commissioner's independence. As a result of the independence, there were additional administrative requirements. The Commissioner's office then requested and received additional funding from the Treasury Board to meet these administrative requirements as well as to provide additional operational support for fulfilling the Commissioner's mandate.

## Comparative study of CSEC and international partners

During the summer of 2009 the Commissioner's office was fortunate to welcome a master's student from Carleton University who completed a comparative study of publicly available information respecting CSEC and some of its international partners, their authorities, activities and oversight and review mechanisms. The study informs work such as the ongoing classified review of CSEC's foreign intelligence sharing with international partners.



---

## Canadian Association of Security and Intelligence Studies (CASIS) conference

In October 2009 staff of the Commissioner's office participated in the annual CASIS conference, held in Ottawa. The theme of the conference was *Terrorism, Cyberspies and a New 'Cold' War: Emerging Challenges for Security and Intelligence*. The conference attracted many leading experts, scholars, policy makers, practitioners and academics from within Canada and internationally. Lectures and panels provided new perspectives on the ever broadening challenges facing the security and intelligence community.

## International Intelligence Review Agencies Conference (IIRAC)

In March 2010, the Executive Director of the Commissioner's office attended the IIRAC in Sydney, Australia, leading a discussion on effective review, with a description of the Commissioner's office's approach in areas such as staff recruitment and development, review targeting and plans, and performance measurement and indicators.

The objectives of the bi-annual IIRAC are to share ideas and best practices and build capacity in the review and oversight functions of participating organizations. Participants are from countries that share basic principles of rule of law and democratic control over security and intelligence agencies. Participating organizations represent many different models of review and oversight, adding to the richness of exchanges of information and experience.

---

## IN CLOSING

(by the Honourable Peter deC. Cory)

I would like to take this opportunity to say a word about Joanne Weeks, who stepped down recently as Executive Director of the Commissioner's office. She had directed the day-to-day business of the office since the appointment of the first Commissioner, the Honourable Claude Bisson, in 1996. Joanne oversaw an important evolution of the office when a legislative framework was provided for both the Commissioner's office and CSEC in the omnibus *Anti-terrorism Act*, following the terrorist attacks of September 11, 2001. For the relatively short time that I worked with Joanne, I came to appreciate her clear devotion to public service and saw her as a generous, warm-hearted individual. Joanne knew the important role that review plays and strove to ensure that she had the most capable staff to carry out the work. As her retirement approaches, I would like to express my sincere appreciation and thanks to Joanne for her dedication, not just to the Office of the CSE Commissioner but, more importantly, to Canada. Her work provides an outstanding example to all in the public service.

## A TRIBUTE TO THE HONOURABLE CHARLES DOHERTY GONTHIER, C.C., Q.C.

(by the Honourable Peter deC. Cory)

The Honourable Charles Doherty Gonthier passed away on July 17, 2009, while still Commissioner of the Communications Security Establishment Canada. Active to the end in service to his country, and applying his intellect with customary vigour, he contributed significantly in many areas of the law. His interest and work in later years dealt with sustainable development, demonstrating a great social conscience and sympathy for vulnerable members of society.

Charles and I were appointed to the Supreme Court of Canada on the same day in 1989. A greatly respected colleague and a close friend, he will be sorely missed. Fortunately, he leaves a rich legacy which will inspire all of us for the rest of our days.



## ANNEX A: MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

### *National Defence Act – Part V.1*

- 273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.
- (2) The duties of the Commissioner are
- (a) to review the activities of the Establishment to ensure that they are in compliance with the law;
  - (b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and
  - (c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.
- (3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.
- (4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.
- (5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

- (6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.
- (7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

[...]

- 273.65** (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.

### *Security of Information Act*

- 15.** (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest. [...]
- (5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following: [...]
- (b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to, [...]
- (ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.



## ANNEX B: CLASSIFIED REPORTS TO THE MINISTER

1. Principal vs. agent status – March 3, 1997 (TOP SECRET)
2. Operational policies with lawfulness implications – February 6, 1998 (SECRET)
3. CSE's activities under \*\*\* – March 5, 1998 (TOP SECRET Codeword/CEO)
4. Internal investigations and complaints – March 10, 1998 (SECRET)
5. CSE's activities under \*\*\* – December 10, 1998 (TOP SECRET/CEO)
6. On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)
7. How we test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)
8. A study of the \*\*\* collection program – November 19, 1999 (TOP SECRET Codeword/CEO)
9. On \*\*\* – December 8, 1999 (TOP SECRET/COMINT)
10. A study of CSE's \*\*\* reporting process — an overview (Phase I) – December 8, 1999 (SECRET/CEO)
11. A study of selection and \*\*\* — an overview – May 10, 2000 (TOP SECRET/CEO)
12. CSE's operational support activities under \*\*\* — follow-up – May 10, 2000 (TOP SECRET/CEO)
13. Internal investigations and complaints — follow-up – May 10, 2000 (SECRET)
14. On findings of an external review of CSE's ITS program – June 15, 2000 (SECRET)
15. CSE's policy system review – September 13, 2000 (TOP SECRET/CEO)

16. A study of the \*\*\* reporting process — \*\*\* (Phase II) – April 6, 2001 (SECRET/CEO)
17. A study of the \*\*\* reporting process — \*\*\* (Phase III) – April 6, 2001 (SECRET/CEO)
18. CSE's participation \*\*\* – August 20, 2001 (TOP SECRET/CEO)
19. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – August 20, 2001 (TOP SECRET/CEO)
20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – August 21, 2002 (SECRET)
21. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* – November 13, 2002 (TOP SECRET/CEO)
22. CSE's \*\*\* activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)
23. Lexicon of CSE definitions – March 26, 2003 (TOP SECRET)
24. CSE's activities pursuant to \*\*\* Ministerial authorizations including \*\*\* – May 20, 2003 (SECRET)
25. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part I – November 6, 2003 (TOP SECRET/COMINT/CEO)
26. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part II – March 15, 2004 (TOP SECRET/COMINT/CEO)
27. A review of CSE's activities conducted under \*\*\* Ministerial authorization – March 19, 2004 (SECRET/CEO)
28. Internal investigations and complaints — follow-up – March 25, 2004 (TOP SECRET/CEO)
29. A review of CSE's activities conducted under 2002 \*\*\* Ministerial authorization – April 19, 2004 (SECRET/CEO)
30. Review of CSE \*\*\* operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)

31. CSE's support to \*\*\* – January 7, 2005 (TOP SECRET/COMINT/CEO)
32. External review of CSE's \*\*\* activities conducted under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)
33. A study of the \*\*\* collection program – March 15, 2005 (TOP SECRET/COMINT/CEO)
34. Report on the activities of CSE's \*\*\* – June 22, 2005 (TOP SECRET)
35. Interim report on CSE's \*\*\* operations conducted under Ministerial authorization – March 2, 2006 (TOP SECRET/COMINT)
36. External review of CSE \*\*\* activities conducted under Ministerial authorization – March 29, 2006 (TOP SECRET/CEO)
37. Review of CSE's foreign intelligence collection in support of the RCMP (Phase II) – June 16, 2006 (TOP SECRET/COMINT/CEO)
38. Review of information technology security activities at a government department under ministerial authorization – December 18, 2006 (TOP SECRET)
39. Review of CSE signals intelligence collection activities conducted under ministerial authorizations (Phase I) – February 20, 2007 (TOP SECRET/COMINT/CEO)
40. Role of the CSE's client relations officers and the Operational Policy Section in the release of personal information – March 31, 2007 (TOP SECRET/COMINT/CEO)
41. Review of information technology security activities at a government department under ministerial authorization – July 20, 2007 (TOP SECRET)
42. Review of CSEC's counter-terrorism activities – October 16, 2007 (TOP SECRET/COMINT/CEO)
43. Review of CSEC's activities carried out under a ministerial directive – January 9, 2008 (TOP SECRET/COMINT/CEO)
44. Review of CSEC's support to CSIS – January 16, 2008 (TOP SECRET/COMINT/CEO)
45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – March 28, 2008 (TOP SECRET/COMINT/CEO)

46. Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians – June 11, 2008 (TOP SECRET/COMINT/CEO)
47. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) – June 11, 2008 (TOP SECRET/COMINT/CEO)
48. Review of disclosure of information about Canadians to Government of Canada clients – November 19, 2008 (TOP SECRET/COMINT/CEO)
49. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) – January 13, 2009 (TOP SECRET/COMINT/CEO)
50. Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) – February 26, 2009 (TOP SECRET/COMINT/CEO)
51. Review of CSEC activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate – March 12, 2009 (TOP SECRET/COMINT Codeword/CEO)
52. Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive – March 12, 2009 (TOP SECRET/COMINT/CEO)
53. Study of CSEC information technology security activities not conducted under ministerial authorization – June 11, 2009 (TOP SECRET/COMINT/CEO)
54. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations and in support of government efforts relating to Afghanistan – January 18, 2010 (TOP SECRET/COMINT/CEO)
55. Regular review of CSEC disclosure of information about Canadians to Government of Canada clients – February 16, 2010 (TOP SECRET/COMINT/CEO)

---

## ANNEX C: STATEMENT OF EXPENDITURES 2009-2010

### Standard Object Summary

Salaries and Wages	\$930,329
Transportation and Telecommunications	35,893
Information	19,319
Professional and Special Services	378,465
Rentals	157,068
Purchased Repairs and Maintenance	457
Materials and Supplies	11,042
<b>Total</b>	<b>\$1,532,573</b>





---

## ANNEX D: HISTORY OF THE OFFICE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT COMMISSIONER

The Office of the Communications Security Establishment Commissioner was created on June 19, 1996, with the appointment of the inaugural Commissioner, the Honourable Claude Bisson, O.C., a former Chief Justice of Québec, who held the position until June 2003. He was succeeded by the late Right Honourable Antonio Lamer, P.C., C.C., C.D., LL.D., D.U., former Chief Justice of Canada, for a term of three years. The Honourable Charles D. Gonthier, C.C., Q.C., who retired as Justice of the Supreme Court of Canada in 2003, was appointed as Commissioner in August 2006, a position he held until his death in July 2009. The Honourable Peter deC. Cory, C.C., C.D., a former Justice of the Supreme Court of Canada, served as Commissioner from December 14, 2009 to March 31, 2010.

For the first six years (from June 1996 to December 2001), the Commissioner carried out his duties under the authority of Orders in Council issued pursuant to Part II of the *Inquiries Act*. During this period, the Commissioner's responsibilities were twofold: to review the activities of the Communications Security Establishment Canada (CSEC) to determine whether they conformed with the laws of Canada; and to receive complaints about CSEC's activities.

Following the terrorist attacks in the United States on September 11, 2001, Parliament adopted the omnibus *Anti-terrorism Act*, which came into force on December 24, 2001. The omnibus *Act* introduced amendments to the *National Defence Act* by adding Part V.1 and creating legislative frameworks for both the Commissioner's office and CSEC. It gave the Commissioner new responsibilities to review activities carried out by CSEC under a ministerial authorization. The legislation also continued the Commissioner's powers under the *Inquiries Act*.

---

The omnibus legislation also introduced the *Security of Information Act*, which replaced the *Official Secrets Act*. This legislation gives the Commissioner specific duties in the event that a person, who would otherwise be permanently bound to secrecy, seeks to defend the release of classified information about CSEC on the grounds that it is in the public interest.

In autumn 2007, a decision was taken that would sever the Commissioner's office's long-standing arrangements with the Privy Council Office for administrative and other support activities. Effective April 1, 2009, the Commissioner's office was granted its own parliamentary appropriation. While the Commissioner continues to provide the Minister of National Defence with his reports, the Commissioner's office is separate from, and not part of, the Department of National Defence.

---

## ANNEX E: ROLE AND MANDATE OF THE COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

The Communications Security Establishment Canada (CSEC) is Canada's national cryptologic agency, providing the Government of Canada with two key services, foreign signals intelligence and information technology security. CSEC also provides technical and operational assistance to federal law enforcement and security agencies.

CSEC's foreign intelligence products and services support government decision-making in the fields of national security, national defence and foreign policy. CSEC's signals intelligence activities relate exclusively to foreign intelligence and are directed by the Government of Canada's intelligence priorities.

CSEC's information technology security products and services enable government departments and agencies to secure their electronic information systems and networks. CSEC also conducts research and development on behalf of the Government of Canada in fields related to communications security.

CSEC's three-part mandate is set out in subsection 273.64(1) of the *National Defence Act*:

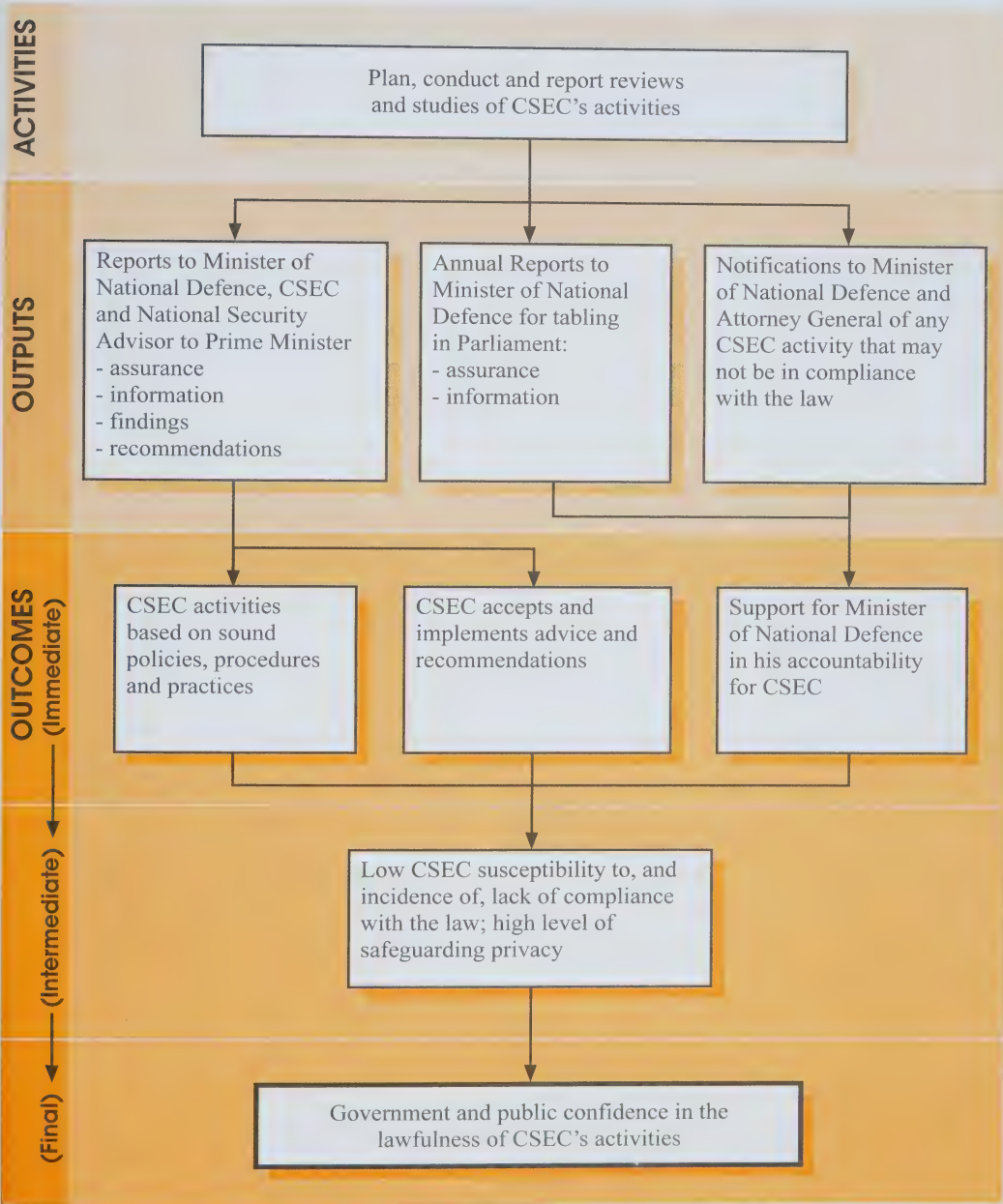
- (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
- (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
- (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.





# ANNEX F: COMMISSIONER'S OFFICE REVIEW PROGRAM — LOGIC MODEL

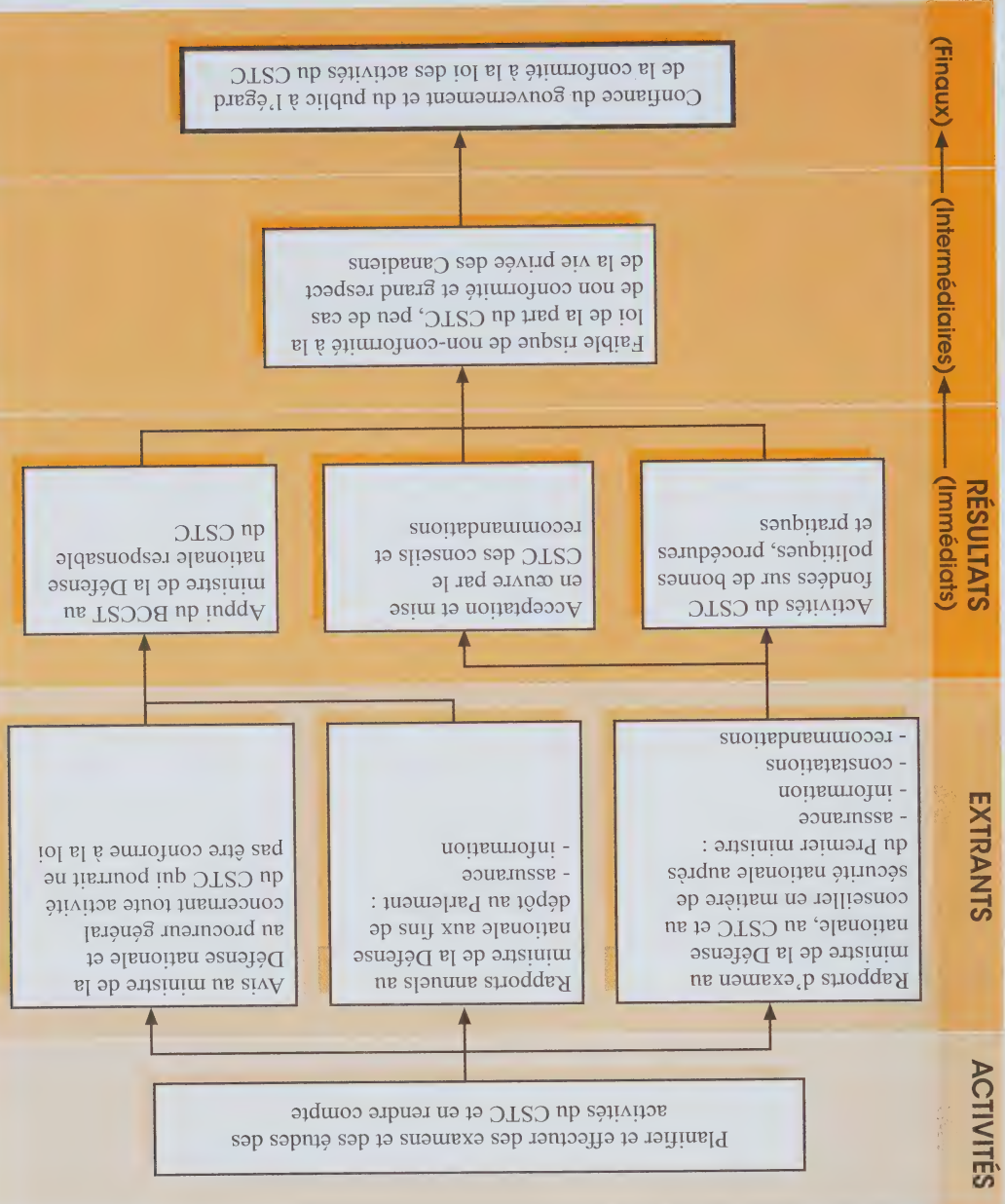
The following logic model provides a graphic description of how the review program functions.







Le modèle logique suivant offre une description graphique de la façon dont le programme d'examen fonctionne.







Le CSTC est l'organisme national de cryptologie du Canada. Organisme unique en son genre au sein de la collectivité canadienne de la sécurité et du renseignement, le CSTC emploie des cryptologues pour protéger la sécurité des technologies de l'information du gouvernement du Canada et lui fournir des renseignements étrangers. Il offre en outre une assistance technique et opérationnelle aux organismes fédéraux chargés de la sécurité et de l'application de la loi.

Les produits et services de renseignement étranger du CSTC sont fournis à l'appui des décisions gouvernementales dans les domaines de la sécurité nationale, du renseignement national et de la politique étrangère. Ses activités en matière de renseignement électromagnétiques visent exclusivement des renseignements étrangers et sont assujetties aux priorités du gouvernement du Canada en matière de renseignement.

Dans le domaine de la sécurité des technologies de l'information, les produits et services du CSTC permettent aux ministères et organismes gouvernementaux d'assurer la sécurité de leurs systèmes et réseaux d'information électronique. Le CSTC effectue aussi des travaux de recherche-développement au nom du gouvernement du Canada dans des disciplines liées à la sécurité des télécommunications.

Le mandat à trois volets du CSTC est établi au paragraphe 273.64(1) de la partie V.1 de la *Loi sur la défense nationale* :

- a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
- b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;
- c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.

En outre, la Loi omnibus a remplacé la Loi sur les secrets officiels par la Loi sur la protection de l'information, laquelle attribue au commissaire des fonctions précises pour les cas où une personne astreinte au secret à perpétuité souhaiterait invoquer la défense de l'intérêt public pour justifier la divulgation de renseignements classifiés sur le CSTC.

Il a été décidé à l'automne 2007 de mettre fin à la relation de longue date que le BCCST entretenait avec le Bureau du Conseil privé pour les fonctions de soutien administratif et autres du bureau. Le BCCST a reçu son propre crédit parlementaire le 1<sup>er</sup> avril 2009. Bien que le commissaire transmette toujours ses rapports au ministre de la Défense nationale, le BCCST est un organisme distinct, ne faisant pas partie de ce ministère.

Le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) a été créé le 19 juin 1996, au moment de la nomination du premier commissaire, l'honorable Claude Bisson, O.C., ancien juge en chef du Québec. M. Bisson a occupé le poste de commissaire jusqu'en juin 2003. Le très honorable Antonio Lamer, c.p., C.C., c.d., LL.D., d.u., ancien juge en chef du Canada (décédé), lui a alors succédé pour un mandat de trois ans. L'honorable Charles D. Gonthier, C.C., c.r., qui a pris sa retraite de la Cour suprême du Canada en 2003, a été nommé commissaire en août 2006 et a occupé cette charge jusqu'à son décès en juillet 2009. L'honorable Peter de C. Cory, C.C., c.d., ancien juge de la Cour suprême du Canada, a occupé la charge de commissaire du 14 décembre 2009 au 31 mars 2010.

Pendant les six premières années de son mandat (de juin 1996 à décembre 2001), le commissaire a exercé ses fonctions conformément à plusieurs décrets, pris en vertu de la partie II de la *Loi sur les enquêtes*. Au cours de cette période, il a assumé une double responsabilité : examiner les activités du Centre de la sécurité des télécommunications Canada (CSTC) afin de déterminer si elles étaient en conformité avec les lois du Canada, et recevoir les plaintes relatives aux activités du CSTC.

Dans le sillage des attentats terroristes du 11 septembre 2001, le Parlement a adopté la *Loi sur la défense nationale*, qui a été promulguée le 24 décembre 2001. Cette Loi modifie la BCCST et du CSTC, et elle confie au commissaire de nouvelles responsabilités relatives à l'examen des activités que mène le CSTC sous le régime d'une autorisation ministérielle. La législation a également confirmé les pouvoirs du commissaire en vertu de la *Loi sur les enquêtes*.



## ANNEXE C : ÉTAT DES DÉPENSES, 2009-2010

### Sommaire des articles courants

Traitements et salaires	930 329 \$
Transports et télécommunications	35 893
Information	19 319
Services professionnels et spéciaux	378 465
Location	157 068
Achat de services de réparation et d'entretien	457
Fournitures et approvisionnements	11 042
<b>Total</b>	<b>1 532 573 \$</b>



45. Review of CSEC signals intelligence collection activities conducted under ministerial authorizations (Phase II) – 28 mars 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
46. Review of CSEC's acquisition and implementation of technologies as a means to protect the privacy of Canadians – 11 juin 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
47. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 1) – 11 juin 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
48. Review of disclosure of information about Canadians to Government of Canada clients – 19 novembre 2008 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
49. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations (Activity 2) – 13 janvier 2009 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
50. Review of CSEC foreign intelligence collection activities conducted under a ministerial directive and ministerial authorizations (Activity 3) – 26 février 2009 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
51. Review of CSEC Activities conducted under a ministerial directive and in support of its foreign intelligence collection mandate – 12 mars 2009 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
52. Follow-up to a recommendation in a 2007–2008 review of CSEC activities carried out under a ministerial directive – 12 mars 2009 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
53. Study of CSEC information technology security activities not conducted under ministerial authorization – 11 juin 2009 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
54. Review of CSEC foreign intelligence collection activities conducted under ministerial authorizations and in support of government efforts relating to Afghanistan – 18 janvier 2010 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
55. Regular review of CSEC disclosure of information about Canadians to Government of Canada clients – 16 février 2010 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

31. CSE's support to \*\*\* – 7 janvier 2005 (TRÈS SECRET/COMINT/  
Réserve aux Canadiens)

32. External review of CSE's \*\*\* activities conducted under Ministerial authorization  
– 28 février 2005 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

33. A study of the \*\*\* collection program – 15 mars 2005 (TRÈS SECRET/  
COMINT/Réserve aux Canadiens)

34. Report on the activities of CSE's \*\*\* – 22 juin 2005 (TRÈS SECRET)

35. Interim report on CSE's \*\*\* operations conducted under Ministerial authorization  
– 2 mars 2006 (TRÈS SECRET/COMINT)

36. External review of CSE \*\*\* activities conducted under Ministerial authorization  
– 29 mars 2006 (TRÈS SECRET/Réserve aux Canadiens)

37. Review of CSE's foreign intelligence collection in support of the RCMP (Phase II)  
– 16 juin 2006 (TRÈS SECRET/COMINT/Réserve aux Canadiens)

38. Review of information technology security activities at a government department  
under ministerial authorization – 18 décembre 2006 (TRÈS SECRET)

39. Review of CSE signals intelligence collection activities conducted under ministerial  
authorizations (Phase I) – 20 février 2007 (TRÈS SECRET/COMINT/  
Réserve aux Canadiens)

40. Role of the CSE's client relations officers and the Operational Policy Section in the  
release of personal information – 31 mars 2007 (TRÈS SECRET/COMINT/  
Réserve aux Canadiens)

41. Review of information technology security activities at a government department  
under ministerial authorization – 20 juillet 2007 (TRÈS SECRET)

42. Review of CSEC's counter-terrorism activities – 16 octobre 2007 (TRÈS SECRET/  
COMINT/Réserve aux Canadiens)

43. Review of CSE's activities carried out under a ministerial directive – 9 janvier 2008  
(TRÈS SECRET/COMINT/Réserve aux Canadiens)

44. Review of CSEC's support to CSIS – 16 janvier 2008 (TRÈS SECRET/COMINT/  
Réserve aux Canadiens)

16. A study of the \*\*\* reporting process — (Phase II) — 6 avril 2001 (SECRET/Réserve aux Canadiens)
17. A study of the \*\*\* reporting process — (Phase III) — 6 avril 2001 (SECRET/Réserve aux Canadiens)
18. CSE's participation \*\*\* — 20 août 2001 (TRÈS SECRET/Réserve aux Canadiens)
19. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — 20 août 2001 (TRÈS SECRET/Réserve aux Canadiens)
20. A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) — 21 août 2002 (SECRET)
21. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — 13 novembre 2002 (TRÈS SECRET/Réserve aux Canadiens)
22. CSE's \*\*\* activities carried out under the \*\*\* 2002 \*\*\* Ministerial authorization — 27 novembre 2002 (TRÈS SECRET/Réserve aux Canadiens)
23. Lexicon of CSE definitions — 26 mars 2003 (TRÈS SECRET)
24. CSE's activities pursuant to \*\*\* Ministerial authorizations including \*\*\* — 20 mai 2003 (SECRET)
25. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part I — 6 novembre 2003 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
26. CSE's support to \*\*\*, as authorized by \*\*\* and code-named \*\*\* — Part II — 15 mars 2004 (TRÈS SECRET/COMINT/Réserve aux Canadiens)
27. A review of CSE's activities conducted under \*\*\* Ministerial authorization — 19 mars 2004 (SECRET/Réserve aux Canadiens)
28. Internal investigations and complaints — follow-up — 25 mars 2004 (TRÈS SECRET/Réserve aux Canadiens)
29. A review of CSE's activities conducted under 2002 \*\*\* Ministerial authorization — 19 avril 2004 (SECRET/Réserve aux Canadiens)
30. Review of CSE \*\*\* operations under Ministerial authorization — 1er juin 2004 (TRÈS SECRET/COMINT)

1. Principal vs. agent status – 3 mars 1997 (TRÈS SECRET)
2. Operational policies with lawfulness implications – 6 février 1998 (SECRET)
3. CSE's activities under \*\*\* – 5 mars 1998 (TRÈS SECRET Mot codé/  
Réserve aux Canadiens)
4. Internal investigations and complaints – 10 mars 1998 (SECRET)
5. CSE's activities under \*\*\* – 10 décembre 1998 (TRÈS SECRET/Réserve aux  
Canadiens)
6. On controlling communications security (COMSEC) material – 6 mai 1999  
(TRÈS SECRET)
7. How we test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière  
de collecte et de conservation de renseignements électromagnétiques, et évaluation  
des efforts de l'organisme pour sauvegarder la vie privée des Canadiens)  
– 14 juin 1999 (TRÈS SECRET Mot codé/Réserve aux Canadiens)
8. A study of the \*\*\* collection program – 19 novembre 1999 (TRÈS SECRET  
Mot codé/Réserve aux Canadiens)
9. On \*\*\* – 8 décembre 1999 (TRÈS SECRET/COMINT)
10. A study of CSE's \*\*\* reporting process — an overview (Phase I) – 8 décembre 1999  
(SECRET/Réserve aux Canadiens)
11. A study of selection and \*\*\* — an overview – 10 mai 2000 (TRÈS SECRET/  
Réserve aux Canadiens)
12. CSE's operational support activities under \*\*\* — follow-up – 10 mai 2000  
(TRÈS SECRET/Réserve aux Canadiens)
13. Internal investigations and complaints — follow-up – 10 mai 2000 (SECRET)
14. On findings of an external review of CSE's ITS program – 15 juin 2000 (SECRET)
15. CSE's policy system review – 13 septembre 2000 (TRÈS SECRET/  
Réserve aux Canadiens)



- (7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.
- [...]
- 273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.
- Loi sur la protection de l'information*
15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public. [...]
- (5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]
- b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession : [...]
- (ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.



273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

- a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;
- b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;
- c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la Loi sur les enquêtes.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.



(Par l'honorable Peter deC. Cory)

J'aimerais profiter de l'occasion pour dire un mot à propos de Joanne Weeks, qui a quitté récemment son poste de directrice exécutive du bureau du commissaire. Joanne, qui dirigeait les activités courantes du bureau depuis la nomination du premier commissaire, l'honorable Claude Bisson, en 1996, a supervisé les remaniements importants du bureau lors de la promulgation de la *Loi antiterroriste* omnibus, dans le sillage des attentats terroristes du 11 septembre 2001, qui l'a dotée, à l'instar du CSTC, d'un cadre législatif. J'ai travaillé relativement peu de temps avec Joanne, mais suffisamment pour me rendre compte de son dévouement à l'égard de la fonction publique et pour voir à quel point il s'agit d'une personne généreuse et chaleureuse. Joanne a conscience du rôle important que joue l'examen et elle s'est efforcée de s'entourer d'une équipe très compétente pour mener à bien ce travail. À la veille de son départ à la retraite, je tiens à lui exprimer mon appréciation et mes sincères remerciements pour son dévouement, non seulement à l'égard du bureau du commissaire du CSTC mais, qui plus est, à l'égard du Canada. Son travail est un exemple remarquable pour tous les membres de la fonction publique.

## HOMMAGE À L'HONORABLE CHARLES DOHERTY GONTHIER, C.C., C.R.

(Par l'honorable Peter deC. Cory)

L'honorable Charles Doherty Gonthier nous a quittés le 17 juillet 2009, alors qu'il était encore commissaire du Centre de la sécurité des télécommunications. Cet homme, qui a continué jusqu'à la fin à servir notre pays, avec toute la vigueur intellectuelle pour laquelle il était reconnu, a fait une contribution importante dans de nombreux domaines du droit. Au cours des dernières années, son travail l'a amené à s'intéresser au développement durable, ce qui lui a permis de donner la pleine mesure de sa conscience sociale et de sa compassion pour les membres les plus vulnérables de la société.

Charles et moi-même avons été nommés à la Cour suprême du Canada le même jour, en 1989. J'ai perdu à la fois un confrère pour qui j'avais le plus profond respect et un ami très cher. Il me manquera énormément. Heureusement, il nous laisse un héritage enviable qui pourra nous inspirer pendant le reste de notre vie.

## Colloque de l'Association canadienne pour les études de renseignement et de sécurité (ACERS)

En octobre 2009, le personnel du bureau du commissaire a participé au colloque annuel de l'ACERS qui s'est tenu à Ottawa. Sous le titre *Terrorisme, cyberespions et nouvelle guerre « froide » : défis émergents pour la sécurité et le renseignement*, le colloque, qui portait sur le terrorisme et l'espionnage informatique, a attiré nombre d'experts éminents, ainsi que des chercheurs, des décideurs, des professionnels et des universitaires de toutes les régions du pays et de l'étranger. Les conférences et les discussions en petits groupes ont livré de nouveaux points de vue sur les défis toujours grandissants que doit relever le milieu du renseignement et de la sécurité.

## Conférence internationale des organismes de surveillance du renseignement

En mars 2010, le directeur exécutif du bureau du commissaire a assisté à la Conférence internationale des organismes de surveillance du renseignement, à Sydney (Australie), où il a animé un débat sur l'examen efficace et décrit l'approche du bureau du commissaire dans des domaines comme le recrutement et le perfectionnement du personnel, le ciblage des examens et les plans, ainsi que la mesure et les indicateurs de rendement. La conférence biennale a pour objet de faire part d'idées, de pratiques exemplaires et de renforcer la capacité des fonctions d'examen et de supervision des organismes participants. Les participants sont issus de pays qui partagent les principes fondamentaux de la règle de droit et du contrôle démocratique sur les organismes voués au renseignement et à la sécurité. Les organismes participants représentent de nombreux modèles différents d'examen et de supervision, ce qui contribue à la richesse des échanges d'information et d'expérience.

## OBLIGATIONS SOUS LE RÉGIME DE LA LOI SUR LA PROTECTION DE L'INFORMATION

Le commissaire est tenu, en vertu de la *Loi sur la protection de l'information*, de recevoir de l'information émanant de personnes astreintes au secret à perpétuité, qui ont l'intention de communiquer des renseignements opérationnels spéciaux en faisant valoir la primauté de l'intérêt public. Aucune affaire de ce genre n'a été signalée au commissaire au cours de la période visée par le rapport.

### LE BUREAU DU COMMISSAIRE

L'an dernier, le bureau du commissaire s'est vu accorder son propre crédit parlementaire, ce qui a renforcé l'indépendance du commissaire. Cette indépendance est assortie de nouvelles exigences administratives. Le bureau du commissaire a alors demandé et reçu un financement additionnel du Conseil du Trésor pour faire face à ces exigences administratives de même que pour assurer un soutien opérationnel complémentaire à l'appui du mandat du commissaire.

### Étude comparative du CSTC et de ses partenaires étrangers

Au cours de l'été 2009, le bureau du commissaire a eu la chance d'accueillir un étudiant à la maîtrise de l'Université Carleton qui a effectué une étude comparative des renseignements accessibles au public concernant le CSTC et certains de ses partenaires étrangers, leurs pouvoirs, leurs activités ainsi que les mécanismes de supervision et d'examen. L'étude éclaire des travaux portant notamment sur l'examen classifié continu de l'échange de renseignements étrangers entre le CSTC et ses partenaires étrangers.



En vertu de son mandat, le commissaire est tenu d'entreprendre toute enquête jugée nécessaire par suite d'une plainte, de façon à déterminer si le CSTC a mené, ou mène une activité non conforme à la loi.

En 2009–2010, de la correspondance concernant des activités du CSTC fut reçue, mais rien dans cette correspondance ne justifiait une enquête.

## PLAINTES CONCERNANT LES ACTIVITÉS DU CSTC

Parmi les autres examens prévus en 2010–2011, mentionnons l'aide apportée au SCRS en vertu de la partie c) du mandat du CSTC et des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*; l'examen annuel de la divulgation par le CSTC de renseignements sur des Canadiens aux clients du gouvernement du Canada et à des partenaires étrangers; la conservation et la destruction des renseignements par le CSTC et, en particulier, les communications et l'information privées sur des Canadiens; et l'aide apportée par le CSTC au SCRS en vertu de la partie c) du mandat du CSTC et des articles 16 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*. Certains examens pourraient être reportés à l'exercice financier 2011–2012.

## Examens à venir

méthode utilisée par le CSTC pour repérer de nouvelles entités susceptibles de livrer des renseignements étrangers d'intérêt; et un examen annuel des autorisations ministérielles relatives aux renseignements étrangers, y compris un échantillon de communications privées connexes.

Le bureau du commissaire choisit les activités du CSTC qui seront visées par un examen et établit un ordre de priorité à partir d'une série de critères détaillés. Par exemple, l'examen continu de l'échange de renseignements étrangers entre le CSTC et ses partenaires étrangers est considéré comme hautement prioritaire. Les raisons sont les suivantes : il y a eu des changements touchant les autorisations et les technologies se rapportant à ces activités; le CSTC et ses partenaires étrangers se transmettent un volume important de renseignements étrangers; ces activités pourraient avoir une incidence directe et néfaste sur ces Canadiens; des contrôles particuliers et importants sont exercés sur ces activités pour assurer la conformité aux exigences juridiques, ministérielles et stratégiques, et il y a lieu d'en vérifier l'application; enfin, dans le cadre des examens antérieurs visant ces activités, les commissaires ont fait des constatations et des recommandations qui exigent un suivi.

## **Examens en cours**

Les résultats de plusieurs examens actuellement en cours devraient faire l'objet d'un rapport au ministre de la Défense nationale dans l'année à venir et ils figureront dans le rapport annuel public 2010-2011 du commissaire. Les sujets de ces examens sont les suivants : échange de renseignements étrangers entre le CSTC et ses partenaires étrangers; activités relatives à la sécurité des TI menées en vertu des autorisations ministérielles; processus en vertu duquel le CSTC détermine que les cibles de renseignements étrangers d'intérêt sont des entités étrangères situées en dehors du territoire canadien, comme l'exige la *Loi sur la défense nationale*; une

Le *Rapport annuel 2008-2009* du commissaire renferme le résumé d'un examen approfondi de la divulgation de renseignements sur des Canadiens aux clients du gouvernement du Canada. Comme l'examen a révélé que les activités du CSTC étaient conformes à la loi ainsi qu'aux politiques et procédures du CSTC, ce dernier a suggéré par la suite que le bureau du commissaire procède à un examen de ce genre à intervalles réguliers. Conscient que cette activité du CSTC constitue un volet important de la protection de la vie privée des Canadiens, l'ancien commissaire Gonthier a accueilli favorablement cette suggestion, et des examens mensuels de toutes les divulgations du CSTC aux clients du gouvernement du Canada ont été effectués de janvier à juin 2009.

## Constatations

Les examens mensuels ont révélé que la divulgation de renseignements par le CSTC concernant des Canadiens dans les rapports sur les renseignements étrangers adressés à des clients du gouvernement du Canada était conforme à la loi ainsi qu'aux politiques et procédures opérationnelles de l'organisme. Comme ces résultats étaient encourageants, il a été déterminé que les examens mensuels n'étaient pas nécessaires et ne constituaient pour aucune des deux parties une utilisation optimale de ses ressources. Toutefois, en raison des conséquences de cette activité sur la protection de la vie privée des Canadiens, à compter de 2010-2011, le commissaire procédera à un examen annuel d'un échantillon aléatoire de divulgations pour vérifier si le CSTC continue de se conformer à la loi et adopte des mesures qui protègent la vie privée des Canadiens.

## Recommandations

Nonobstant les constatations positives, l'ancien commissaire Gonthier a formulé deux recommandations relatives à l'obligation de rapporter au ministre de la Défense nationale portant sur le volume de renseignements concernant des Canadiens transmis à des clients du CSTC. Les recommandations demandent que l'on fournisse des outils à l'appui du repérage de ces renseignements et de l'amélioration de la cohérence et de l'exactitude du rapport. Le CSTC a souscrit aux recommandations et il s'emploie à les mettre en œuvre.

modifie sa politique visant ces activités pour clarifier certaines obligations. Le fait que le CSTC ait donné suite à cette recommandation, renforçant ainsi sa capacité de s'acquiescer des exigences juridiques et ministérielles, constitue un point positif. Le bureau du commissaire surveillera par ailleurs les efforts du CSTC pour combler les lacunes relatives à ces activités dans ses interactions avec les Forces canadiennes, comme l'ont indiqué les évaluateurs internes du CSTC.

En outre, l'examen rend compte de deux améliorations apportées par le CSTC en ce qui concerne les rapports sur la collecte de renseignements étrangers qu'il convient de faire valoir. D'abord, le CSTC a pris des mesures pour centraliser la gestion d'un certain type de rapport propre à améliorer la reddition de comptes. Ensuite, le CSTC a donné suite à une recommandation formulée par l'ancien commissaire Gonthier, demandant que l'on consigne, en vue d'en faire rapport au ministre de la Défense nationale, des renseignements complémentaires concernant les activités de collecte de renseignements étrangers à l'appui de la reddition de comptes.

## Examen périodique de la divulgation par le CSTC de renseignements sur des Canadiens aux clients du gouvernement du Canada

### Contexte

Cet examen a été amorcé et effectué sous l'autorité de l'ancien commissaire Gonthier, aux termes de l'alinéa 273.63(2)a) de la *Loi sur la défense nationale*. Le rapport a été examiné et présenté au ministre de la Défense nationale par l'ancien commissaire Cory.

Sur réception d'une demande de divulgation de détails concernant des renseignements supprimés à propos d'un Canadien dans un rapport, le CSTC exige que le client rende compte de son pouvoir de demander et d'utiliser ces renseignements dans le cadre de son mandat et qu'il fournisse une justification opérationnelle de son besoin de connaître. Le CSTC ne transmet les renseignements supprimés qu'une fois que ces conditions ont été remplies.



En attendant les modifications pour clarifier la *Loi sur la défense nationale*, cet examen est fondé sur l'interprétation juridique des dispositions relatives à l'autorisation ministérielle applicable aux renseignements stipulés dans la *Loi sur la défense nationale*, fournie au CSTC par le ministère de la Justice du Canada.

Comme il s'agissait du premier examen de ces activités, le but était d'acquérir une connaissance détaillée des activités, d'évaluer si elles étaient autorisées et conformes à la loi, et de déterminer dans quelle mesure le CSTC protégeait la vie privée des Canadiens dans le cadre de ces activités.

## Constatations

Il est clair que les activités du CSTC déployées en vertu d'une autorisation ministérielle et relatives à l'Afghanistan permettent à l'organisme d'avoir un accès important à des renseignements étrangers fort précieux à l'appui des priorités du renseignement de l'armée et du gouvernement en général.

L'examen a révélé que les activités avaient donné accès à un très petit nombre de communications et d'information privées sur des Canadiens. Tout indique par conséquent qu'elles présentent un faible risque pour la vie privée des Canadiens.

D'après l'information dépouillée et les entrevues, les activités menées par le CSTC en vertu d'une autorisation ministérielle de 2006 à 2008 et se rapportant à l'Afghanistan étaient dûment autorisées et ont été menées en conformité avec la loi et les avis du ministère de la Justice du Canada. Tout indique que ces activités respectaient également les exigences des autorisations et des instructions ministérielles. Le CSTC a consigné et transmis l'information au ministre conformément aux exigences énoncées dans les autorisations.

## Recommandations

Rien dans l'information ou la documentation n'indiquait que les employés du CSTC ont contrevenu aux politiques et procédures opérationnelles applicables aux activités de collecte de renseignements étrangers. Toutefois, l'ancien commissaire Gonthier a recommandé que le CSTC



Cet examen a été amorcé et réalisé sous l'autorité de l'ancien commissaire Gonthier, aux termes des dispositions du paragraphe 273.65(8) de la *Loi sur la défense nationale*. Le rapport a été examiné et présenté au ministre de la Défense nationale par l'ancien commissaire Cory. L'examen portait sur les activités menées en vertu de deux autorisations ministérielles en vigueur en 2006-2007 et en 2007-2008 et à l'appui des opérations militaires des Forces canadiennes et des autres efforts gouvernementaux relatifs à l'Afghanistan. Le CSTC a obtenu les autorisations ministérielles en vertu des paragraphes 273.65(1) et (2) de la *Loi sur la défense nationale* du fait qu'au cours de ses activités, il était possible qu'il intercepte une communication entamée ou terminée au Canada et constituant une communication privée au sens du *Code criminel*.

## Examen d'activités de collecte de renseignements étrangers entreprises par le CSTC en vertu d'autorisations ministérielles et à l'appui des efforts gouvernementaux en Afghanistan

L'étude portait également sur l'examen d'un outil logiciel essentiel du CSTC pour la sécurité des TI et d'un dépôt central des sources d'information. L'ancien commissaire Gonthier a conclu que l'outil logiciel du CSTC relatif à la sécurité des TI comportait une fonction adéquate pour restreindre l'accès à l'information stockée dans le système, satisfaisant aux exigences de sécurité et de confidentialité et protégeant la vie privée des Canadiens. Pour confirmer ce constat, le bureau du commissaire a examiné l'utilisation du système par le CSTC dans le contexte de l'examen de certaines activités relatives à la sécurité des TI menées en vertu d'une autorisation ministérielle. Les résultats de cet examen figureront dans le rapport annuel de 2010-2011.

## Surveillance des systèmes de détection des intrusions

L'alinéa 184(2)e) du *Code criminel* autorise l'interception d'une

communication privée par une personne ayant le contrôle d'un système

informatique de façon à protéger ce système contre tout acte qui

constituerait une infraction aux termes du paragraphe 342.1(1) (utilisation

non autorisée d'ordinateur) ou du paragraphe 430(1.1) (méfait concernant

les données) du *Code criminel*. Cette disposition autorise le recours à un

système de détection des intrusions pour protéger l'ordinateur contre une

cyber-attaque et permet d'utiliser ou de conserver la communication privée

interceptée lorsqu'elle est essentielle pour détecter, isoler ou empêcher des

activités dommageables pour le système informatique.

L'article 161 de la *Loi sur la gestion des finances publiques* investit une entité

gouvernementale du pouvoir de prendre des mesures raisonnables pour

protéger un système informatique, notamment l'interception d'une

communication privée dans les circonstances précisées à l'alinéa 184(2)e)

du *Code criminel*.

Canadiens. Ces activités se déroulent sous l'égide d'autres entités

gouvernementales, en vertu du *Code criminel* et de la *Loi sur la gestion*

des *finances publiques*, et peuvent permettre au CSTC d'avoir accès à des

communications et à de l'information privées sur des Canadiens. En ce qui

concerne ces activités, il appert que le CSTC prend des mesures pour

protéger la vie privée des Canadiens. Par exemple, les communications et

l'information privées sur des Canadiens ne sont divulguées qu'aux agents

chargés de la protection des systèmes informatiques. Néanmoins, il existe

bel et bien un risque pour la vie privée. Par conséquent, le bureau du

commissaire effectuera des examens approfondis de ces activités pour

vérifier la conformité du CSTC et pour évaluer dans quelle mesure il

protège la vie privée des Canadiens en menant ces activités.

TI et à gérer les risques afférents. Cela peut nécessiter des activités de veille et des parades pour prévenir et détecter les menaces et les cyber-attaques, ou y réagir.

Les objectifs de l'étude consistaient à prendre connaissance des activités du CSTC relatives à la sécurité des TI et à effectuer une évaluation du risque pour déterminer lesquelles peuvent, le cas échéant, poser un problème pour la conformité à la loi, aux exigences ministérielles ou aux politiques et procédures du CSTC, ou la protection de la vie privée des Canadiens — et devraient par conséquent faire l'objet d'un examen de suivi. Une attention particulière a été accordée aux activités qui peuvent viser des communications ou des renseignements privés sur des Canadiens.

L'étude a porté sur les domaines suivants : programme de chiffrage du gouvernement du Canada; relations avec l'industrie; recherche, analyse et rapports concernant la vulnérabilité à la criminalité informatique et menaces et attaques complexes visant les TI; aide pour recenser les vulnérabilités et les incidents touchant les infrastructures d'information importantes pour le gouvernement, ainsi que pour trouver des parades; et relations connexes avec les partenaires clés du gouvernement canadien et ses partenaires étrangers.

## Constatations et conclusions

L'étude a révélé que les activités du CSTC relatives à la sécurité des TI non menées en vertu d'une autorisation ministérielle présentent généralement un faible risque de non-conformité à la partie V.1 de la *Loi sur la défense nationale* et un faible risque également pour la vie privée des Canadiens. Le quart des questions visées par l'étude fera l'objet d'un examen de suivi et a été intégré au plan de travail triennal du commissaire. Dans quelques rares cas seulement, les activités du CSTC relatives à la sécurité des TI non menées en vertu d'une autorisation ministérielle donnent accès à une petite quantité de renseignements sur des Canadiens. La plupart se rapportent à l'identité d'une société canadienne ou consistent en des renseignements fournis volontairement par les clients gouvernementaux du CSTC dans le cadre des activités de cybersécurité ou des affaires courantes de l'État. Il y a toutefois d'autres activités relatives à la sécurité des TI non menées en vertu d'une autorisation ministérielle qui peuvent présenter des risques pour la vie privée des

Le commissaire présente des rapports classifiés renfermant ses constatations et ses recommandations au ministre de la Défense nationale, et il en remet copie au chef du CSTC, au conseiller en matière de sécurité nationale auprès du Premier ministre, qui rend compte des opérations et de la politique du CSTC, et au sous-ministre de la Défense nationale, qui rend compte des questions administratives se rapportant au CSTC. Avant de finaliser un rapport, le bureau du commissaire recueille les commentaires du CSTC concernant l'exactitude des faits qui y sont mentionnés.

## Étude des activités relatives à la sécurité des technologies de l'information qui ne sont pas menées en vertu d'une autorisation ministérielle

### Contexte

Cette étude a été lancée et réalisée sous l'autorité de l'ancien commissaire Gonthier, aux termes de l'alinéa 273.63(2)a) de la *Loi sur la défense nationale*. Elle porte sur les activités du CSTC relatives à la sécurité des technologies de l'information (TI) qui ne sont pas menées en vertu d'une autorisation ministérielle. Un examen des activités relatives à la sécurité des TI avait déjà été effectué en 2000. Toutefois, en raison de changements et de progrès importants sur ce front depuis cette date, une étude approfondie s'imposait. Les autres activités relatives à la sécurité des TI que mène le CSTC en vertu d'une autorisation ministérielle sont examinées annuellement.

En matière de sécurité des TI, le CSTC tire sa légitimité de l'alinéa 273.64(1)b) de la *Loi sur la défense nationale* qui stipule que le CSTC a pour mandat de : « Fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada ». Les activités du CSTC relatives à la sécurité des TI visent à prévenir les menaces et les cyber-attaques complexes visant les TI qui pourraient permettre à des intrus d'avoir accès secrètement aux systèmes informatiques sensibles du gouvernement. Il incombe également au CSTC de réagir aux menaces ou attaques de ce genre. Entre autres activités relatives à la sécurité des TI, le CSTC fait la promotion de saines pratiques de sécurité pour aider les ministères fédéraux à réduire la vulnérabilité des



Outre l'approche de l'examen horizontal, le bureau du commissaire examine désormais chaque année toutes les autorisations ministérielles de collecte de renseignements étrangers d'une manière regroupée. Cet examen met en évidence tout changement important dans les activités visées par les autorisations ministérielles ou à l'intérieur d'une autorisation. Tout changement important fait l'objet d'une évaluation sous l'angle des risques pour la conformité et pour la vie privée des Canadiens. Le cas échéant, on effectuera un examen détaillé. Cet examen annuel des autorisations ministérielles portera également sur les communications privées interceptées qui ont été utilisées et conservées, et l'on s'assure qu'il s'agit bel et bien de communications essentielles aux affaires internationales, à la défense, ou à la sécurité du Canada, comme l'exige l'alinéa 273.65(2)d) de la *Loi sur la défense nationale*.

## Raison d'être d'un examen horizontal

Fruit des années d'expérience du bureau du commissaire en matière d'examen, l'examen horizontal vise à donner au personnel du bureau une vision encore plus détaillée de la façon dont le CSTC mène ses activités. À terme, l'objectif est d'accroître le degré d'assurance que peut offrir le commissaire au ministre de la Défense nationale concernant la conformité du CSTC à la loi et la protection de la vie privée des Canadiens.

Plutôt que d'examiner de manière approfondie les autorisations ministérielles de façon individuelle, on a jugé plus efficace d'analyser de manière approfondie chaque procédure commune aux activités de collecte de renseignements étrangers visées par une autorisation ministérielle. Cette nouvelle approche, qui transcende les méthodes de collecte, est appelée *examen horizontal*.



**Exigences ministérielles** — Le commissaire s'attend à ce que le CSTC

mène chaque activité d'une manière qui est en accord avec les instructions ministérielles, à savoir toute exigence ou limite précisée dans une autorisation ou des directives ministérielles.

**Politiques et procédures** — Le commissaire s'attend à ce que le CSTC dispose de politiques et de procédures pertinentes pour orienter ses activités et donner des consignes suffisamment claires concernant les obligations en vertu de la loi, les exigences ministérielles et la protection de la vie privée des Canadiens. Le commissaire s'attend à ce que les employés du CSTC soient au courant des politiques et procédures et qu'ils s'y conforment. Le commissaire s'attend également à ce que le CSTC utilise un cadre de contrôle de gestion efficace pour donner l'assurance qu'il n'y a pas de faille dans l'intégrité et la conformité à la loi de ses activités. Il s'agit notamment de l'obligation de rendre compte des décisions prises et de l'information relative à la conformité et à la protection de la vie privée des Canadiens.

**Une nouvelle approche pour examiner les activités de collecte de renseignements étrangers**

Les activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une autorisation ministérielle ont recours à plusieurs méthodes distinctes d'acquisition d'information à partir de l'infrastructure mondiale d'information. Néanmoins, il y a plusieurs processus communs et outils communs, de même que des bases de données et systèmes communs qui appuient ces méthodes de collecte et auxquels le CSTC fait appel pour traiter les renseignements obtenus. Par exemple, les éléments communs à l'ensemble des méthodes de collecte sont les processus par lesquels le CSTC : choisit les entités étrangères situées à l'extérieur du Canada qui présentent un intérêt pour la collecte de renseignements étrangers; partage les rapports et l'information avec ses clients et partenaires étrangers; et garde ou détruit les communications interceptées.

Dans le cadre de ses examens, le personnel du commissaire passe en revue tous les documents pertinents – dossiers, fichiers, correspondance et autres documents écrits et électroniques, y compris les politiques, procédures et avis juridiques. En plus de présenter des exposés et des démonstrations de ses activités, le CSTC répond de manière détaillée aux questions écrites du bureau du commissaire. Outre qu'il a la possibilité de vérifier l'information obtenue en faisant des comparaisons avec le contenu des systèmes et bases de données du CSTC, le personnel du commissaire s'entretient avec les gestionnaires du CSTC et d'autres membres du personnel participant aux activités visées par l'examen et observe directement les opérateurs et les analystes pour comprendre exactement comment ils effectuent leur travail.

Le bureau du commissaire peut également se reporter au travail des vérificateurs et des évaluateurs internes du CSTC. Dans certains cas, cela peut l'amener à repérer une activité sur laquelle il se penchera.

## Critères d'examen

Les examens menés par le bureau du commissaire comportent une évaluation des activités du CSTC par rapport à une série de critères standard concernant les obligations en vertu de la loi, les exigences ministérielles ainsi que les politiques et procédures du CSTC. D'autres critères peuvent être ajoutés à chaque examen, selon les besoins.

### Obligations en vertu de la loi — Le commissaire s'attend à ce que le

CSTC mène chaque activité en conformité avec la *Loi sur la défense nationale*, la *Charte canadienne des droits et libertés*, la *Loi sur la protection des renseignements personnels*, le *Code criminel*, et toute autre législation pertinente ainsi que les avis du ministère de la Justice du Canada.

**la conformité**

Les commissaires s'attachent à privilégier les pratiques exemplaires propres à maintenir ou à renforcer la conformité du CSTC à la loi et la protection de la vie privée des Canadiens. Le CSTC a continué à apporter des améliorations notables à ses pratiques de gestion de l'information et à utiliser davantage son système de gestion des dossiers. Par le passé, ces enjeux ont fait l'objet de recommandations des commissaires. Ces améliorations sont essentielles pour la reddition de comptes et la conformité du CSTC.

Il faut également féliciter le CSTC pour une nouvelle initiative qui vise à mieux sensibiliser les employés et à leur faire connaître les autorisations, politiques et procédures régissant ses activités. Grâce à cette initiative, chaque employé a désormais accès en ligne aux politiques qui se rapportent expressément à son poste. L'initiative devrait renforcer le cadre de conformité du CSTC et la protection de la vie privée des Canadiens.

**Conditions préalables à un degré d'assurance supérieur**

Au cours de l'exercice écoulé, le CSTC a présenté plusieurs exposés détaillés au personnel du bureau du commissaire. Certains, de nature générale, avaient pour but de tenir le bureau informé de ses problèmes opérationnels, organisationnels ou stratégiques, et d'autres visaient à donner des précisions sur des activités particulières du CSTC avant d'établir le cahier des charges en vue d'un examen ou pendant un examen en cours. Plusieurs exposés décrivaient les outils, systèmes et bases de données du CSTC, y compris ceux utilisés par l'organisme afin de se conformer aux exigences de la loi dans le ciblage des entités étrangères à l'extérieur du Canada.

Les exposés, ainsi qu'un accès direct aux systèmes du CSTC et aux employés de première ligne, ont permis au bureau du commissaire d'effectuer un examen plus approfondi en 2009-2010. Dans l'ensemble, il a pu assurer avec certitude au ministre de la Défense nationale que le CSTC se conforme à la loi et protège la vie privée des Canadiens.

**Renforcement de la reddition de comptes et de la conformité**

## Examen régulier de la divulgation de renseignements sur les Canadiens

Dans le rapport annuel du commissaire pour l'année 2008-2009, il fut remarqué que le bureau du commissaire effectuerait régulièrement des examens de la divulgation de renseignements sur des Canadiens aux clients du gouvernement du Canada. Pendant une période de six mois au cours de l'exercice écoulé, le bureau du commissaire a effectué des examens mensuels de toutes les divulgations et il a estimé qu'elles étaient conformes à la loi ainsi qu'aux politiques et procédures du CSTC. Compte tenu de ces résultats positifs et du résultat convaincant d'un examen plus approfondi des divulgations dont rend compte le rapport annuel 2008-2009, il a été déterminé que des examens mensuels n'étaient pas nécessaires. Toutefois, puisque cette activité du CSTC est au cœur du mandat du commissaire, comme le faisait observer l'ancien commissaire Gonthier l'an dernier, un examen sera encore effectué sur une base annuelle.

## Délais des réponses du CSTC aux demandes d'information

En 2009-2010 plusieurs facteurs extraordinaires et pressions extérieures ont eu une incidence sur les opérations du CSTC, dont la nécessité de donner suite à des événements spéciaux sur la scène internationale. Si les commissaires ne s'objectent pas au principe selon lequel les opérations du CSTC demeurent la priorité de l'organisme, le CSTC parfois a mis beaucoup trop de temps à répondre aux demandes d'information du bureau du commissaire au cours de l'exercice écoulé. Le CSTC se penche sur les moyens qu'il pourrait déployer pour mieux se conformer aux exigences du commissaire en matière d'examen.



L'exercice écoulé qui fait l'objet du rapport a été une année exceptionnelle pour le bureau du commissaire. Comme nous l'avons mentionné dans l'introduction, le bureau a été privé de commissaire Gonthier, mais il a continué d'accomplir son travail. Les examens et les rapports classifiés ont été achevés et d'autres, qui avaient été approuvés par l'ancien commissaire Gonthier, se sont poursuivis ou ont été amorcés comme prévu.

L'objectif premier des examens consiste à évaluer si les activités du CSTC sont conformes à la loi et dans quelle mesure des dispositions adéquates sont en place pour protéger la vie privée des Canadiens. Trois rapports classifiés ont été présentés au ministre au cours de l'exercice écoulé. L'un était une étude approfondie se rapportant aux activités du CSTC relatives à la sécurité des technologies de l'information et les deux autres étaient des examens se rapportant aux activités de renseignement étranger.

Les deux examens ont révélé que le CSTC s'est conforme à la loi et aux exigences ministérielles et qu'il a protégé la vie privée des Canadiens. Le CSTC a souscrit aux recommandations formulées dans les examens et il prend actuellement des mesures pour y donner suite. Le CSTC se penche également sur les constatations afin d'améliorer ses politiques ou pratiques.

### Mise en œuvre des recommandations

Depuis 1997, les commissaires ont présenté au ministre de la Défense nationale 55 études et rapports d'examen classifiés. Au total, ces rapports renferment 129 recommandations. Le CSTC a accepté et mis en œuvre ou s'emploie à mettre en œuvre 94 p. 100 (121) de ces recommandations. Les rares recommandations qui n'ont pas été acceptées ou mises en œuvre portent sur des questions devenues désuètes au fil des événements ou des circonstances. Lorsque le CSTC rejette une recommandation, le commissaire analyse les raisons qui motivent la décision, détermine si elles sont acceptables ou s'il y a lieu d'insister, le cas échéant, en approfondissant encore la question.



Concernant le rôle des membres du Parlement, et dans le contexte de l'élaboration d'un meilleur cadre de sécurité nationale, la réponse du gouvernement faisait part de son intention d'accorder toute l'attention requise à la cinquième recommandation formulée par le Comité permanent de la sécurité publique et nationale voulant que le projet de loi C-81, *Loi constituant le Comité de parlementaires sur la sécurité nationale*, présente lors de la 38<sup>e</sup> législature, ou une variante de ce projet de loi, soit présenté au Parlement dans les plus brefs délais. Les anciens commissaires se sont interrogés sur la composition d'un tel comité et sur son accès à des renseignements de sécurité nationale classifiés.

Les commissions d'enquête O'Connor et Iacobucci ont également soulevé plusieurs questions concernant l'échange d'information entre les organismes canadiens voués à la sécurité et au renseignement et des organismes étrangers. La réponse du gouvernement indiquait que « les résultats cumulatifs des commissions d'enquête successives, des rapports et des leçons apprises ont mené à l'amélioration des politiques et des pratiques relatives à l'échange d'information entre les partenaires étrangers et les communautés canadiennes de la sécurité nationale, du renseignement et de l'application de la loi ». L'échange d'information constitue un élément essentiel du programme de renseignement étranger du CSTC. Le bureau du commissaire effectuée à l'heure actuelle l'examen de cette activité.

Dans sa réponse aux recommandations des commissions d'enquête O'Connor et Iacobucci, le gouvernement a indiqué qu'il continuerait de tenir compte de l'avis des intervenants. Le bureau du commissaire est prêt à débattre de ces questions.

En 2010-2011, le bureau du commissaire effectuera un examen de l'assistance du CSTC à l'appui du SCRS ayant trait à l'interception de communications au Canada provenant de Canadiens situés à l'étranger. sous réserve d'un mandat en vertu des articles 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité, dans des conditions identiques à la demande autorisée par la décision du juge Mosley.

## Constatations et recommandations découlant des commissions d'enquête Iacobucci et O'Connor

En juin 2009, le Comité permanent de la sécurité publique et nationale a publié un rapport faisant état de son étude des constats et recommandations de l'Enquête interne sur les actions des responsables canadiens relativement à Abdullah Almaliki, Ahmad Abou-Elmaati et Muayyed Nureddin (enquête Iacobucci) ainsi que du rapport de la Commission d'enquête sur les actions des responsables canadiens *relativement à Maher Arar* (enquête O'Connor). Le Comité permanent a exhorté le gouvernement à mettre en œuvre toutes les recommandations de ces commissions d'enquête.

En octobre 2009, le gouvernement a répondu au rapport du Comité permanent en faisant part de sa détermination «... à moderniser et à renforcer le cadre d'examen des activités de sécurité nationale au Canada», et en précisant que «[l]e gouvernement a pour objectif de renforcer les structures d'examen existantes...» et que «[d]es progrès importants ont été accomplis à l'égard de l'analyse des politiques touchant le cadre d'examen des activités de sécurité nationale du Canada, plus particulièrement... l'établissement d'un mécanisme pour faciliter les examens interorganisme des activités de sécurité nationale.»

En ce qui concerne ce dernier point, l'ancien commissaire Gonthier estimait qu'il n'y avait pas d'obstacle, ni juridique ou autre, à la coopération entre les organismes d'examen de la sécurité nationale, et qu'on avait tout à gagner en menant des examens conjoints ou parallèles, ainsi que des travaux de recherche ou d'autres missions en collaboration.

# Aide du CSTC au Service canadien du renseignement de sécurité (SCRS), en vertu de la partie c) du mandat du CSTC et des articles 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité

Les questions de sécurité nationale font de plus en plus l'objet de procédures devant les tribunaux et d'autres procédures publiques. Dans sa décision du 5 octobre 2009 sur une demande de mandat en vertu des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité*, l'honorable juge Mosley de la Cour fédérale a autorisé le SCRS, avec l'aide technique du CSTC, à intercepter des communications au Canada se rapportant à des activités que deux personnes, selon des allégations, allaient mener au cours d'un voyage à l'étranger, et qui constitueraient une menace pour la sécurité. Le juge Mosley a établi une distinction entre cette demande et une autre demande similaire entendue en octobre 2007 par l'honorable juge Blanchard, également de la Cour fédérale.

Dans les motifs de la décision, le juge Mosley dit ce qui suit : « en autorisant le SCRS, avec le soutien technique du CSTC, à obtenir des renseignements ... interceptés au Canada, je n'autorise pas le CSTC à outrepasser le mandat légal que lui confie la *Loi sur la défense nationale*. [...] Les activités du CSTC ne visent pas des citoyens canadiens et n'auront pas pour but d'obtenir des renseignements pour le CSTC, elles serviront plutôt à aider le SCRS ».

## Mandat du CSTC pour aider les organismes fédéraux chargés de l'application de la loi et de la sécurité

L'alinéa 273.64(1)c) de la *Loi sur la défense nationale* autorise le CSTC à fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère. Le CSTC est assujéti à toutes restrictions imposées par la loi visant l'organisme auquel il fournit son assistance — par exemple, les conditions imposées par un juge dans un mandat.



## Communications privées et information concernant des Canadiens

Les examens des activités menées par le CSTC en vertu d'autorisations ministérielles ont montré invariablement que la proportion de communications privées de Canadiens qu'intercepte par inadvertance le CSTC est très petite.

Les rapports classifiés sur les renseignements étrangers du CSTC peuvent renfermer de l'information sur des citoyens canadiens, des résidents permanents ou des sociétés canadiennes (en vertu de l'article 273.61 de la *Loi sur la défense nationale*), si cette information est jugée essentielle à la compréhension de l'ensemble. Toutefois, l'information doit être supprimée, c'est-à-dire qu'elle est remplacée par une mention générale du type « un Canadien ou une Canadienne ».

Les autorisations ministérielles concernant les renseignements étrangers du CSTC sont rédigées de façon très générale et s'appliquent aux méthodes de collecte des renseignements étrangers plutôt qu'aux personnes. Toutefois, de l'avis des commissaires, il n'apparaît pas clairement que la *Loi sur la défense nationale* appuie une telle approche. Ils préconisent donc que l'on apporte des modifications à la *Loi sur la défense nationale* pour clarifier les ambiguïtés relatives aux autorisations ministérielles visant les renseignements étrangers. Ainsi, l'ancien commissaire Gonthier a réitéré l'an dernier que « le temps qui s'écoule sans qu'on applique les modifications législatives met en danger l'intégrité du processus d'examen. »

Le commissaire Gonthier a été informé par le ministre de la Défense nationale du fait que la levée des ambiguïtés et d'autres modifications à la *Loi sur la défense nationale* constituent une priorité législative. En attendant les modifications, les commissaires ont continué d'avoir recours à une solution provisoire, qui consiste à émettre une opinion avec réserve, c'est-à-dire examiner les activités de collecte de renseignements étrangers menées par le CSTC en vertu d'une autorisation ministérielle en fonction de l'interprétation de la *Loi sur la défense nationale* par le ministère de la Justice du Canada. Toutefois, les anciens commissaires ont signifié leur désaccord à l'égard de certains aspects importants de cette interprétation, ce qui attire l'attention sur la nécessité d'apporter des modifications à la *Loi sur la défense nationale*.

Le mandat dont est investi le commissaire en vertu de la loi consiste notamment à examiner les activités du CSTC menées en vertu des autorisations ministérielles pour s'assurer qu'elles ont été autorisées et exécutées en conformité avec la loi. Les examens menés par les anciens commissaires n'ont jamais mis au jour de situation où le CSTC aurait ciblé les communications d'un Canadien ou d'une personne vivant au Canada.

- aux politiques et procédures du CSTC.
- l'autorisation ministérielle; et
- le ministre concernant certaines informations après l'expiration de des raisons de reddition de comptes, d'enregistrement et de rapport au l'autorisation ou dans des instructions ministérielles, par exemple, pour aux exigences établies par le ministre de la Défense nationale dans
- ministère de la Justice du Canada;
- à la législation pertinente, à savoir la *Loi sur la défense nationale*, la *Charte canadienne des droits et libertés*, la *Loi sur la protection des renseignements personnels*, le *Code criminel*, de même que l'avis du
- doivent être entreprises conformément :

Les activités du CSTC menées en vertu d'une autorisation ministérielle technologies de l'information (paragraphe 273.65 (4)).

de conditions visent les autorisations ministérielles relatives à la sécurité des de collecte de renseignements étrangers (paragraphe 273.65 (2)) et cinq Quatre conditions sont stipulées concernant les autorisations ministérielles conditions établies dans la *Loi sur la défense nationale* sont remplies.

ministre de la Défense nationale doit être convaincu que certaines communications privées. Toutefois, avant d'accorder cette autorisation, le ministre de la Défense nationale à autoriser le CSTC à intercepter des Reconnaissant cette possibilité, la *Loi sur la défense nationale* permet au



Cela ne veut pas dire qu'il n'y a pas eu ou qu'il ne peut y avoir des points de désaccord. Mais il est possible de travailler plus efficacement à les résoudre du fait que le personnel du CSTC possède une connaissance approfondie de la loi et une connaissance pratique de la façon dont elle s'applique à son travail.

Pour finir, permettez-moi de dire qu'après ma nomination à la fin de 2009, plusieurs événements se sont produits qui m'ont amené à écarter mon mandat en tant que commissaire. Il s'agit de circonstances que je regrette profondément, d'autant plus que le processus de sélection prend du temps. On rencontre parfois des situations dans la vie où les choses ne tournent pas comme on l'aurait cru ou voulu. Quoi qu'il en soit, je suis reconnaissant de la possibilité qui m'a été donnée de travailler avec le personnel compétent et consciencieux du bureau du commissaire. Nul doute à mes yeux que mon successeur disposera d'une assise solide sur laquelle s'appuyer pour assumer la charge importante et indépendante de commissaire, laquelle consiste à garantir que le CSTC respecte la loi et protège la vie privée des Canadiens dans l'exercice du mandat dont il est investi.

## CONTEXTE DE L'EXAMEN

### Modifications proposées à la loi sur la défense nationale

*La Loi sur la défense nationale* interdit que les activités du CSTC relatives à la collecte de renseignements étrangers et à la sécurité des technologies de l'information visent un Canadien ou une personne vivant au Canada. Elle exige en outre que le CSTC prenne des mesures pour protéger la vie privée des Canadiens concernant l'utilisation et la conservation des renseignements interceptés.

Toutefois, en raison de la manière dont les communications sont transmises, le CSTC peut, tout en s'acquittant de la collecte de renseignements étrangers ou en menant ses activités relatives à la sécurité des technologies de l'information, comme l'exige son mandat, intercepter par inadvertance des communications des Canadiens ou des personnes vivant au Canada, qui sont des « communications privées » au sens de l'article 183 du *Code criminel*.

C'est avec plaisir que j'ai accepté la charge de commissaire du Centre de la sécurité des télécommunications, où je suis entré en fonction le 14 décembre 2009. Le bureau était privé de commissaire depuis le décès, en juillet dernier, de mon prédécesseur et ancien confrère à la Cour suprême du Canada, feu l'honorable Charles D. Gonthier.

À mon arrivée au bureau, en décembre dernier, j'ai été immédiatement impressionné par le professionnalisme et le dévouement du personnel. Malgré l'absence de commissaire entre le décès de M. Gonthier et ma nomination, le travail s'était poursuivi, et le personnel avait procédé à l'examen des activités du Centre de la sécurité des télécommunications Canada (CSTC). Le suivi des rapports d'examen au ministre, qui relève exclusivement du commissaire, était la seule tâche demeurée en attente.

J'ai aussi été frappé par le professionnalisme et le dévouement du personnel du CSTC. Le travail à l'appui des Forces canadiennes stationnées en Afghanistan, qui constitue une priorité du gouvernement du Canada et permet parfois de sauver des vies, m'apparaît un domaine d'activité de la plus haute importance pour le CSTC en 2009-2010.

Au cours de la période qui s'est écoulée entre ma nomination et la fin de la période visée par le rapport, j'ai acquis une connaissance approfondie des activités du CSTC grâce aux explications détaillées du chef du CSTC de même qu'aux explications et aux discussions avec mon personnel concernant l'examen des activités du CSTC pour évaluer la conformité à la législation pertinente.

Je sais d'après les rapports précédents que les activités du CSTC passées en revue étaient conformes à la loi. Les discussions que j'ai eues avec le chef du CSTC et avec mon personnel ont fait ressortir la cohérence avec laquelle le CSTC s'acquitte de son mandat. Les activités sur lesquelles j'ai présenté des rapports au ministre de la Défense nationale étaient également conformes à la loi. Ce constat témoigne de l'éthique de la conformité qui existe au sein du CSTC.

Le bureau du commissaire /23

- Etude comparative du CSTC et de ses partenaires étrangers 23
- Colloque de l'Association canadienne pour les études de renseignement et de sécurité (ACERS) /24
- Conférence internationale des organismes de surveillance du renseignement 24

Pour conclure /25

Hommage à l'honorable Charles Doherty Gonthier, C.C., c.r. 25

Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications /27

Annexe B : Rapports classifiés au ministre /29

Annexe C : Etat des dépenses, 2009-2010 /33

Annexe D : Historique du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) /35

Annexe E : Rôle et mandat du Centre de la sécurité des télécommunications Canada (CSTC) /37

Annexe F : Programme d'examen du BCCST – Modèle logique /39

- Modifications proposées à la Loi sur la défense nationale / 2
- Aide du CSTC au Service canadien du renseignement de sécurité (SCRS), en vertu de la partie c) du mandat du CSTC et des articles 12 et 21 de la Loi sur le Service canadien du renseignement de sécurité / 5
- Constatations et recommandations découlant des commissions d'enquête Iacobucci et O'Connor / 6

- Examen régulier de la divulgation de renseignements sur les Canadiens / 9
- Délais des réponses du CSTC aux demandes d'information / 9
- Conditions préalables à un degré d'assurance supérieur / 10
- Renforcement de la reddition de comptes et de la conformité / 10

- Critères d'examen / 11
- Une nouvelle approche pour examiner les activités de collecte de renseignements étrangers / 12

- Étude des activités relatives à la sécurité des technologies de l'information qui ne sont pas menées en vertu d'une autorisation ministérielle / 14
- Examen d'activités de collecte de renseignements étrangers entreprises par le CSTC en vertu d'autorisations ministérielles et à l'appui des efforts gouvernementaux en Afghanistan / 17
- Examen périodique de la divulgation par le CSTC de renseignements sur des Canadiens aux clients du gouvernement du Canada / 19

- Examens en cours / 21
- Examens à venir / 22

1928-2009

l'honorable Charles D. Gonthier, C.C., c.r.

*Ce rapport est dédié à la mémoire de*



13674

Commissaire du Centre de la  
sécurité des télécommunications

L'honorable Robert Décary, c.r.



CANADA

Communications Security  
Establishment Commissioner

The Honourable Robert Décary, Q.C.

Juin 2010

Ministre de la Défense nationale  
Edifice MGen G.R. Pearkes, 13<sup>e</sup> étage  
101, promenade Colonel-By, tour nord  
Ottawa (Ontario)  
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63(3) de la *Loi sur la défense nationale*, j'ai l'honneur de vous transmettre le rapport annuel pour la période allant du 1<sup>er</sup> avril 2009 au 31 mars 2010, faisant état des activités et des constatations de mes deux prédécesseurs, l'honorable Peter deC. Cory et l'honorable Charles D. Gonthier, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Le commissaire,

A handwritten signature in dark ink, appearing to read "Robert Décary".

Robert Décary

P.O. Box/C.P. 1984, Station "B"/Succursale « B »  
Ottawa, Canada  
K1P 5R5  
(613) 992-3044 Téléc.: (613) 992-4096

Bureau du commissaire du Centre  
de la sécurité des télécommunications  
C.P. 1984, Succursale « B »  
Ottawa (Ontario)  
K1P 5R5

Tél. : (613) 992-3044  
Télé. : (613) 992-4096  
Site Web : [www.ocsec-bccst.gc.ca](http://www.ocsec-bccst.gc.ca)

© Ministre des Travaux publics et des  
Services gouvernementaux Canada 2010  
ISBN 978-1-100-51826-8  
N° de cat. D95-2010

Photos de la couverture : Malak



Canada

2009-2010



# Rapport annuel

COMMISSAIRE  
DU CENTRE  
DE LA SÉCURITÉ  
DES TÉLÉCOMMUNICATIONS













